PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 | A2

(11) International Publication Number: **WO 99/21319**

(43) International Publication Date: 29 April 1999 (29.04.99)

(21) International Application Number: PCT/US98/22377

(22) International Filing Date: 21 October 1998 (21.10.98)

(30) Priority Data:

60/062,630	22 October 1997 (22.10.97)	US
09/175,927	21 October 1998 (21.10.98)	US

(71) Applicant: INTERX TECHNOLOGIES, INC. [US/US]; Suite H, 1805 Tribute Road, Sacramento, CA 95815 (US).

(72) Inventors: ABDALLAH, Wajdi; 5400 Garfield #46, Sacramento, CA 95841-2856 (US). DALMATOFF, Adam; 2765 Larkspur Lane, Sacramento, CA 95864 (US).

(74) Agents: GLENN, Michael, A. et al.; Law Offices of Michael A. Glenn, 125 Lake Road, Portola Valley, CA 94028 (US).

(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GD, GE, HR, HU, ID, IL, IS, JP, KP, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, UZ, VN, YU, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: METHOD AND APPARATUS FOR CERTIFICATE MANAGEMENT IN SUPPORT OF NON-REPUDIATION

(57) Abstract

A non-repudiation mechanism for e-business is provided. E-business covers three areas: Intranet, Extranet, and E-commerce. The invention provides a link between a server which sends Internet requests to the requesting browser, and the application which houses the data and any computing functions. An audit trail is also provided to fix accountability. The invention controls the session between the server and the e-business application. The result is that each and every system request made via Internet technology can be correlated to a specific system user. Management utilities and reports provide the audit trail which provides non-repudiation (accountability).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR CERTIFICATE MANAGEMENT IN SUPPORT OF NON-REPUDIATION

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to electronic information. More particularly, the invention relates to electronic information security.

DESCRIPTION OF THE PRIOR ART

Technology and business developments have created tremendous opportunities for companies to lower costs and improve customer service and satisfaction in the past several years. Visionary organizations have recognized the need to create new communication methods to maintain industry leadership and support their customers' changing purchasing processes. The Internet has the potential to make electronic commerce more practical, as many organizations have already discovered. Explosive exponential growth doubles the rate of Internet use every 100 days (see *The Emerging Digital Economy*, U.S. Department of Commerce, April 1998 (www.ecommerce.gov/emerging.htm)), much faster than previous communication technologies have been adopted. Opportunities abound: organizations of all types are competing for customers by offering compelling and convenient new services. Small companies now can effectively compete against rivals with much larger budgets. In turn, this has spurred cross-industry battles for market share in this new high-tech medium. Businesses and organizations worldwide desire to extend product and service offerings via the Internet and World Wide Web, however, high security and liability risks often stand in the way.

The major concern restraining the use of the Internet as a medium for electronic commerce is application security. It is estimated that US Department of Defense systems suffered 250,000 attacks in 1995, and 63% of these attacks were both successful and

undetected (see U.S. Senator Sam Nunn, Speech at Georgia Institute of Technology, April 6, 1998). Although no classified systems or records are admitted to having been penetrated, accounting, administration, and logistical systems were accessed. These are the same systems that in the corporate and financial world are responsible for communications, transactions, and audit.

To further complicate Internet security, more than 50% of all intrusions occur from within an organization (see *1996 Computer Crime and Security Survey*, Computer Security Institute (www.gocsi.com)) and the most serious losses occur from internal sources as well (see *1998 Computer Crime and Security Survey*, Computer Security Institute (www.gocsi.com)). The need to control access of permitted users and the establishment of a verifiable audit over the Internet is paramount for true security. The current environment lacks these capabilities and curtails expansion and automation of full-fledged eBusiness. However, opportunities are so great for both the private and public sectors that security risks are outweighed by lower costs, speed to market and extended reach. Even without factoring in future improved Internet security mechanisms, Web based commerce is expected to reach $300 billion by 2002 for business-to-business transactions alone (see *The Emerging Digital Economy*, US Department of Commerce, April 1998 (www.ecommerce.gov/emerging.htm)). Once sensitive, high value, and real time processing security requirements are addressed, there is no telling how fast or how high Internet transaction values will grow.

> "...So what is needed, I think, is obvious to all – security. What is less discussed is the need to bind a system of trust to the security systems. This is the only way that security will be truly achieved. ...security is concerned with locks, fences, and guards. Trust is about whether they work. In network terms, security is not just about encryption. ...but also is about authentication, digital signatures, data integrity, and non-repudiation. Trust is about key management, digital certificates, and policy – such as what your privileges are, what you are authorized or not authorized to do with your digital signature.
>
> ...we cannot keep building new capabilities on a poor foundation of security. ...It is folly to hope that someday we can add needed elements

before it's too late. The longer we wait, ...the costlier it will be to address the problem.

We share the same network with our adversaries. We are staking our future on a resource that we have not yet learned to protect. Meanwhile, if our security remains where it is now, the risks and costs of attacking us will keep getting lower. ...the solutions depend on trust."

George J. Tenet, Director of US Central Intelligence at the Nations Bank Policy Forum, April 6, 1998 (the full text of George J. Tenet's speech "Information Security Risks, Opportunities, and the Bottom Line" is available at http://www.odci.gov/cia/public_affairs/ speeches/dci_speech_040698.html).

SUMMARY OF THE INVENTION

The invention provides a system that binds trust over the Internet, and enables real time Internet transactions and audit, while addressing security concerns and requirements. The invention provides simplified authentication and authorization to users and administrators alike, and establishes a single sign-on mechanism for all Internet applications. Thus, the invention changes the dynamics of the Internet and establishes evidence that connects identity with activity, or, non-repudiation. The invention provides security and audit capabilities that meet or exceed US and Internationally mandated banking regulations and standards (see Federal Deposit Insurance Corp. (www.fdic.gov), Bank of International Settlements (www.bis.ch)), and, it uses only standard Internet technology to do so (see National Institute of Standards and Technology (www.nist.gov), International Standards Organization (www.iso.ch), and Internet Engineering Task Force (www.ietf.org)). As a result, the invention provides a system that fits easily into existing and newly created business environments and leverages both existing technology investments and business strategies.

Return on investment can be realized quickly with the invention in multiple implementation scenarios. Large and small organizations alike can secure Internet communications and manage Internet, Intranet and Extranet access rights enterprise-wide. Reduced start-up and operating costs offer greater opportunities for retail, business, and

government trade, while the Internet provides the cost-effective communications mechanism. As an organization continues to grow, time to market and the production cost of new services can be reduced by integrating the invention as the security, access, and audit technology into user applications and solutions.

The invention is completely transparent and conforms itself to existing business rules and processes. The Internet provides the low cost and ubiquitous network, and the invention provides the security, control, and audit requirements that reduce fraud, theft, and misuse, while encouraging and providing for increased and higher value information exchange.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block schematic diagram showing a comparison between an OSI and a TCP/IP network model;

Fig. 2 is a block schematic diagram showing system architecture components according to the invention;

Fig. 3 is a block schematic diagram showing inter-relation of the system architecture components shown in Fig. 2;

Fig. 4 is a block schematic diagram showing functions and information flows according to the invention;

Fig. 5 is a block schematic diagram showing a context model according to the invention;

Fig. 6 is a data flow diagram according to the invention;

Fig. 7 is a block schematic diagram showing an Internet billing application context model according to the invention;

Fig. 8 is a block schematic diagram showing an Internet billing application process and data model according to the invention;

Fig. 9 is a block schematic diagram showing functional decomposition of an Internet billing application according to the invention;

Fig. 10 is a block schematic diagram showing functional decomposition of an Internet bill payment and presentment application according to the invention; and

Fig. 11 is a block schematic diagram of a network segmentation model according to the invention.

DETAILED DESCRIPTION OF THE INVENTION

The invention is preferably situated between a server and whatever information a user is trying to access. The invention manages and coordinates all HTTP traffic coming through the server and imposes the security and access rules which the owner of the system has associated with each user and each URI. For purposes of the discussion herein, URI is a URL plus everything that comes after the delimiter ".com."

Without the invention, records can be kept at the Web server and records can be kept at the application, but the types of data kept on each are different and there is no way to connect the two into a continuous audit trail. Without the invention, two different sets of records can be compared, and any discrepancies remain discrepancies because there is no method of reconciliation or audit. The invention forms the link between the server and the application/URI, and establishes a continuous audit trail that can be used to enforce accountability.

The following is an everyday use scenario of a high security site using Digital IDs and passwords for security and access control as it is today without the invention:

1. User requests information from database application.

2. Server requests digital identification.

3. User submits Digital ID.

4. Server receives Digital ID.

5. For example, the ID is accepted and the user is allowed access to the application.

6. The application asks for user name/password.

7. The user submits user name and password.

8. The application checks user name and password and, if all is in order, the user is allowed access to application/information.

Thus, the application and the server are working independently. The application does not know which user or which ID has been allowed access to its log-in screen. The application accepts any valid username/password without reference to the digital ID.

With the foregoing prior art approach, the result (for example) for a person working at a bank who happens to know/find another employees username/password can access the application by submitting their digital ID to the server and the other individual's username/password to the application to be given access. The vagaries of http and the World Wide Web do not allow for accountability of system users. If the bank finds a discrepancy, it can come to the person who used another's username/password and the person can say that she was not logged into the application. In fact, this person could be logged in elsewhere and showing other activities at the same time. If the bank comes to the employee signed into the application, that person can say she was not logged in with her digital ID to the server.

The invention provides the mechanism to connect the server and the application to form continuous and unbroken, reconcilable and auditable audit trails that establish accountability of system users. The invention creates for http communications what is possible for security and audit in a client/server or mainframe application. The invention performs its processes and functions for each and every data request.

Thus, the invention provides a system that binds trust over the Internet, and enables real time Internet transactions and audit, while addressing security concerns and requirements. The invention provides simplified authentication and authorization to users and administrators alike, and establishes a single sign-on mechanism for all Internet applications. Thus, the invention changes the dynamics of the Internet and establishes evidence that connects identity with activity, or, non-repudiation. The invention provides security and audit capabilities that meet or exceed US and Internationally mandated banking regulations and standards (see Federal Deposit Insurance Corp. (www.fdic.gov), Bank of International Settlements (www.bis.ch)), and, it uses only standard Internet technology to do so (see National Institute of Standards and Technology (www.nist.gov), International Standards Organization (www.iso.ch), and Internet Engineering Task Force

(www.ietf.org)). As a result, the invention provides a system that fits easily into existing and newly created business environments and leverages both existing technology investments and business strategies.

Return on investment can be realized quickly with the invention in multiple implementation scenarios. Large and small organizations alike can secure Internet communications and manage Internet, Intranet and Extranet access rights enterprise-wide. Reduced start-up and operating costs offer greater opportunities for retail, business, and government trade, while the Internet provides the cost-effective communications mechanism. As an organization continues to grow, time to market and the production cost of new services can be reduced by integrating the invention as the security, access, and audit technology into user applications and solutions.

The invention is completely transparent and conforms itself to existing business rules and processes. The Internet provides the low cost and ubiquitous network, and the invention provides the security, control, and audit requirements that reduce fraud, theft, and misuse, while encouraging and providing for increased and higher value information exchange.

System Components

The preferred embodiment of the invention uses digital signatures, authentication, access control, data integrity, and non-repudiation to accomplish Web based security, control, and audit. This creates an environment of system trust. When these security features are processed by the invention, the Internet with all its potential as a reliable commercial marketplace is established.

The preferred embodiment of the invention fits as a layer between the Internet and user resources that are to be protected and controlled. The invention is completely configurable and designed to integrate into existing application environments to enable such environments for secure Internet eCommerce. The invention provides a system that is flexible, *i.e.* it delivers security, control, and audit capabilities to any Internet application with any business or communication function. Providers of online products and services who extend trust to customers, clients, employees, and/or administrators can provide security and non-repudiation without complicating ease of use. The invention allows exchanging purchase orders, invoices, bid request, legal documents, medical

records, and financial data, all with common Internet technology in standard merchant to consumer, and business-to-business processes and formats. The invention provides a system that manages the components identified below to secure and control Internet connected systems and networks.

- **Digital Signatures** are unique pieces of technology that are used to identify people or machines. Many different kinds of digital signatures, or digital IDs (DID) exist including SmartCards, biometrics, and digital certificates, which are most often used for Internet identification schemes. The invention can be integrated to be used with any DID, but for purposes of this document the discussion herein concentrates on digital certificates. Once a reliable and unique certificate is issued to a user's customers, business associates, and employees, the invention uses this certificate to identify the person requesting services from the user's system, and tracks their actions throughout their stay. Digital signatures enable proof positive identification over the Internet.

- **Authentication** functions in the invention have a unique multi-layer design to offer superior security values for an Internet connected environment. The invention provides a system that enforces authentication for each and every action requested from each user without negatively impacting system performance. The invention performs authentication checks for both local and third party DID issuers to confirm validity and establish identity. DID and password configurations not using the invention only check these security measures at log on. In contrast thereto, the invention does this continuously. Additionally, the DID and password execute their authentication at separate and unconnected locations in the user's system. The invention binds digital certificates and password together and asks for authorization, as with an ATM card. This link separates security provided by the invention, and enables real time secure communications and transactions over the Internet. To distinguish authentication further, a second layer of authentication can be enabled to enforce challenge questions if the user's security assessment requires extremely strict measures.

- **Access Control** in the invention provides the ease of single Internet, Intranet, and Extranet sign-on without compromising security or application utility. Access control and authorization are used to control the information and applications which individuals

and groups are permitted to access. Due to the nature of Web technology, standard Internet access control mechanisms operate only at the start of communications, but the invention provides a system that performs this function continuously for every request made to a user's system. Access control permits a sales person to access only the accounts they manage, while the sales manager can access the accounts of all the sales employees. At the same time, neither can access human resources or accounting data. The invention permits full control of access to all system users based upon their role in an organization. Additional control is provided to set access rights by time, frequency, and number of visits to a specific location, thus enabling controlled product and service distribution. The invention allows control over the sequence in which information is requested as well. This feature, taken for granted in a non-Internet system, further distinguishes access control and security provided by the invention.

- **Data Integrity** is a crucial element in system security and has the added benefit of providing privacy to communications as well. It ensures that the information sent and received is unaltered. The invention provides a system that handles data integrity functions with cryptography. The invention provides protection for online communication and for data residing on the system itself. Thus, the invention prevents its own system data from being altered by only permitting it to be viewed. This is a key element in maintaining non-repudiation. Data integrity is crucial to proving that information has not been tampered with in cases of legal or company policy enforcement.

- **Non-repudiation** is the capability to thwart repudiation and provides the basis for proving the identity behind each and every action made to a user's system through the Internet, Intranet, or Extranet. The invention provides a system that enables clear reports that form a complete and unbroken audit trail and establishes the same accepted level of proof that is possible with non-Internet systems. This unbroken Internet audit trail is what enables a protected and managed system to provide sensitive and high value information. The invention thus frees companies from the constraints of Web technology and allows product and service distribution.

- **Monitoring and alarms** provide mechanisms to further protect a user's valuable information systems. The invention provides a system that permits alarms to be

configured should illegal or improper activities be discovered. Alarms can be set to cut communications, suspend access rights and page security personnel. The invention also maintains the records so hackers can be found and prosecuted.

The invention provides easy integration into existing technology systems and business processes. This allows control of all aspects of Internet, Intranet, and Extranet communications so that a user's system reflects the user's precise security, control, and audit requirements. Simple configuration screens allow for access control and flow control that can be managed by individual, group, application, file, page, date, or time, even exception handling is available. Complete monitoring and reporting data can be standardized for Internet connections streamlining security, audit, and policy management enterprise-wide. The invention operates in the background, transparent to the user. The results are non-transparent, Internet technology with the addition of security and accountability.

Unified Administration

The invention helps quicken return on investment because management, training, and audit requirements can be centralized and standardized, and existing technology investments are leveraged. Policies and procedures for maintenance, security, and audit are designed to integrate easily into a user's existing corporate culture, as they are fully configurable. A single set of Internet access policies and procedures can be established, which both strengthens and simplifies security.

The invention is fully expandable. As new applications are developed or brought online, the invention's administration features simplify the introduction into a user's organization. There are no limits as to how many applications can be protected. The invention effectively secures and connects a user's organization with Web technology inside and out.

Extranet and Virtual Private Network

Extranet use of the invention lets trading partners use the Internet to communicate with a user through a standard Netscape or Microsoft browser. The invention provides a

system that is seamless and transparent. There is nothing to come between a user's customers and the ease of use that the Internet provides. All traditional merchant to consumer functions can be provided and carried out with confidence. Because there is no software to distribute, education and support costs are low. Customers also benefit from strong identification, and the security that any confidential data about them cannot be unknowingly misused.

The invention extends business-to-business transactions to even the smallest organizations as VAN functions can take place over an enabled Virtual Private Network (VPN). Installing the invention at both ends of an Internet transmission establishes a VPN with all the access and cost savings inherent with the Internet. VPN implementations incorporating the invention are stronger than standard VPN installations because security is executed at the Internet application itself. The invention is preferably situated between a user's business applications and the Internet. Other VPNs establish security between the network and the Internet and cannot establish accountability at the application. VPNs that incorporate the invention can process data in real time on the Internet with full accountability, and therefore meet the non-repudiation value of a WAN and VAN. Companies previously unable to afford the advantage of automated eCommerce systems can now be targeted for these services.

Intranet

The invention provides a system that allows a user's corporate Intranet to enable employees to work under the same security and controls as found in LAN environments. Workgroup accountability is established, and the universal browser interface streamlines task processing. As employees change departments or move up in the ranks, cumbersome and costly retraining is held to a minimum. A user's staff can even access the user's system from remote locations without requiring the user to support remote access servers or use a VPN.

The invention binds trust to Web applications and delivers continuous security to Web communications for all system users. Application owners get accountability among system users, and a mechanism that permits Internet activities to be audited with detail and non-repudiation. Any application can be made secure for the Internet. Developers

can quicken time to market for future projects by incorporating the invention's security and access control functions into their solutions.

Technical Overview

HTTP lacks the basics of security provisions (identification, authentication, authorization, data integrity, confidentiality, and non-repudiation). Today, HTTP developers must solve these programmatically as part of the HTTP application, but with the invention all of these security provisions are provided to the developer, and are prerequisites for secure HTTP application services.

The invention incorporates many advanced security features into HTTP. Digital certificates and user names are bound together, rather than operating individually thereby mimicking an ATM machine. Beyond securing the application from unauthorized users, the invention tracks all activities of all users establishing accountability of system users and HTTP non-repudiation. Security provisions are isolated from the application, thereby making application development less costly. Additionally, no additional servers are required to take advantage of the invention's powerful security functions.

One of the invention's objectives is to provide an improved HTTP security architecture that allows a user to concentrate on the HTTP application functions. The invention provides the following security functions that developers are normally required to provide to secure HTTP applications:

- Client Identification;
- Digital Certificate Validation;
- Data Encryption;
- Client Authentication;
- Client Authorization;

- Session Management;
- HTTP Application Dispatching;
- Extensive Logging Facilities for Non-repudiation;
- Exception Handling; and
- System Administration and Maintenance.

The following section describes in detail and how the invention can be applied by developers.

Approach

Fig. 1 is a block schematic diagram showing a comparison between an OSI and a TCP/IP network model. The Open System Interconnect (OSI) model 10 was developed by the International Standards Organization (ISO – www.iso.ch), the primary standard-setting body for data communications. Seven layers are defined to provide service subsets for LAN systems. This approach allows groups of related services to be implemented in modules, and makes designing network software more flexible. The OSI model enables an environment where network users and providers can communicate in an atmosphere of trust and accountability. The names and functions of these layers are described below:

1. Physical Layer 11: Defines the electrical, mechanical, and physical interfaces to the network.

2. Data Link Layer 12: Controls the movement of data along the physical network layers. Flow control and error detection is addressed here.

3. Network Layer 13: Addresses and routes packets throughout the network.

4. Transport Layer 14: Provides transparent packet transfer mechanism between systems.

5. Session Layer 15: Establishes, manages, synchronizes and terminates session dialogues.

6. Presentation Layer 16: Encoding and decoding, compression and decompression, and encryption and decryption are handled here.

7. Application Layer 17: Provides standardized network interfacing for end user applications.

DARPA (U.S. Defense Advanced Research Projects Agency, www.darpa.mil) developed the TCP/IP network model 20. The last layer 18 of the TCP/IP network model combines session, presentation, and application functions (*e.g.* mail transmission, login, video, and World Wide Web). HTTP is the application layer protocol in the TCP/IP model that handles Web communication. When comparing these models it is evident that session and presentation responsibilities fall to the application layer. HTTP does not have any distinct presentation or session Layer control mechanisms.

The absence of a separate and distinct session layer in HTTP makes control of Internet traffic (*i.e.* system users and requests) impossible, and results in an insecure and stateless network. The lack of a separate and distinct presentation layer for Internet communications further erodes security and impacts data integrity adversely as well. To establish trust and accountability over the Internet, session and presentation functions must be continuously enforced through the HTTP protocol and into the application itself. Presentation and session control is an integral part in building and maintaining secured and controlled applications for industry and enterprise.

The invention addresses HTTP application security concerns. The invention provides a system in the form of middle-ware that is located between the HTTP server and the application. This approach provides presentation and session control for the HTTP protocol. Thus, the invention provides identification, authentication, authorization, access control, and non-repudiation capabilities for application users.

System Architecture

The invention can be viewed as a collection of interoperable, logical, system components that implement necessary security services to HTTP applications. Fig. 2 is a block schematic diagram showing system architecture components within an Internet environment according to the invention. As shown in Fig. 2 the key logical system components of system architecture are:

- End User Desktop Computer 21;
- Certificate Authority 22 or an Organization's internal Certificate Issuance Department;
- An Organization using the invention 23, 24 (typically including a firewall 30 between the organization and the Internet 29), including:
- Policies and Procedures 25;
- A WWW Server 26;
- A System Application 27; and
- An HTTP Application 28.

Fig. 3 is a block schematic diagram showing inter-relation of the system architecture components shown in Fig. 2. The invention's architecture components are based on the following definitions in a secure HTTP application environment.

1. **End User** 21: A person with a need for a product or service available from a Service Provider Organization (SPO) 23, 24, who meets this need by interacting with an

application through a SPO's Internet/Intranet/Extranet Web site using a desktop computer or other device which supports secure Internet browsing.

2. **Business Associates, Clients, and Partner Entities** 31: An entity that interacts with a SPO using a secure communication channel. This is accomplished when using Internet technology and the invention, which establishes a virtual private network for sending messages, product specifications, purchase orders, invoices, employee data, health records, all of which are highly sensitive and valuable data sets.

3. **Certificate Authority** 22: An organization trusted by a SPO to issue digital signatures to persons and/or machines wishing to communicate with the SPO's HTTP system.

4. **Service Provider Organization** 23, 24: An organization that has an electronic product or service that fulfills end user and/or entity demand. The SPO including the following elements:

- **WWW Server** 26: Software that responds to incoming requests and initiates a secure connection using cryptographic mechanisms.

- **System Application** 27: Software which identifies, authenticates, authorizes, and establishes HTTP user sessions, controls application flow, and tracks the end user and/or entity requests throughout a communication session.

- **Internet based Application** 28: Software with functions that attend to end user and/or entity requests for services and/or products.

- **Back Office System** 32: The internal business processes and information systems infrastructure of a service provider organization.

- **Policies and Procedures** 25: Rules that govern the interaction of people with the network to ensure security and compliance with established business processes.

System Standards

The invention is built based on existing standards (see Table 1 below) to maximize interoperability and reduce costs. The system preferably requires technology standards that are centered upon the need for HTTP based applications to achieve the same security levels found in client/server environments. The standards shown in Table 1 are only examples and are provided for purposes of illustrating the presently preferred embodiment of the invention. They are not intended to be limiting with regard to the scope of the invention.

Table 1: Standards Used by the Invention

Purpose	Standard
Network Communication	The Internet protocol TCP/IP
Application User Interface	HTTP and HTML, as specified by the W3C
Public Key Certificates and Certificate Authority	PKCS X.509 V3
Secure Internet Communication	SSL V3
Cryptography	RSA, DES

Network Communication

The commercial expansion of the Internet has led to enormous interest in developing enterprise Internet based applications. The Internet is the most widely used and lowest cost communication method. Specifically, Internet-based technologies deliver:

- Universal access;
- Instant worldwide distribution;

- Cost effective information exchange and transaction medium; and

- Interoperability, *i.e.* platform independent software and services.

Graphical User Interface

An application user interface must be easy to use from the user's perspective and any necessary software must be easy to deploy and support as well. World Wide Web browsers exist for a variety of platforms and are supported on desktop computers. Browser software is becoming the standard for displaying application information on user desktops. The invention supports the Hypertext Markup Language (HTML), as specified by the W3C. The recommended browser software is either Netscape Navigator V3.0 or later or Microsoft Internet Explorer V3.0 or later, although other browsers may be used in conjunction with the invention.

Public Key Certificates & Certificate Authority

One aspect of the invention relies on public key certificates for identification and authentication of individuals, organization, and machines. The certificates can be issued either by the organization using the invention, or a third party, such as a certificate authority using PKCS, to ensure a unique signature for non-repudiation. These certificates are based on the X.509 V3 standard in the presently preferred embodiment of the invention.

The invention does not limit the number of issuers that can be simultaneously used to manage Internet communications. European clients can use certificates issued by a trusted European authority, American clients through a trusted U.S. authority, while a company's employees worldwide use company issued certificates. The invention works with all the certificate authorities that business processes require.

Secure Internet Communication

There are many ways of securing communications between TCP/IP hosts, specifically between WWW servers and browsers. For generic secure communications

between Web servers and/or browsers, including those requiring strict levels of security, the specified protocol is SSL V3. SSL is the standard of the Internet Engineering Task Force (IETF) and is in common use. This protocol covers the widest range of potential implementations of network software components. No additional software is required to use a standard Web browser (*e.g.* Netscape, Microsoft).

Cryptography

The presently preferred embodiment of the invention uses RSA and DES algorithms and their tool kits to assure that non-repudiation is maintained.

System Functions

Developing security software requires strict coding and communication measures. For this reason the invention minimizes dependencies on APIs for developer use. The invention provides a system that establishes and maintains HTTP application security without limiting or constricting services to be offered on the Web. To achieve these goals and provide flexibility the invention permits detailed and easily changeable encrypted configurations in place of APIs.

The invention provides a security architecture for any HTTP application and is completely effective in stand alone systems, as well as those connected to a corporate back-office system. Each application protected by the invention is passed parameters based upon individually established configurations. All parameters are enabled, disabled, and customized per application, per system function, per user, and per administrator. The security architecture structures the invention's capabilities into platforms, models, options, and customizations.

Fig. 4 is a block schematic diagram showing functions and information flows according to the invention. A detailed description of each function follows:

1. **Engine** 40. The system engine is the controller of system operations which are based on administration configurations. The primary activities of the system engine are:

- Read system configuration from the database at startup;

- Handle client requests;
- Encryption of all data in both database and memory;
- Reserve, manage, and protect memory for its operation and all functions;
- Instruct each function how to perform based upon system configuration;
- Invoke functions based on user request status;
- Construct and manage current user packets;
- Log-out page;
- User change password facility;
- Send parameters and format to the application; and
- Construct the application parameters according to the previous step.

2. **Identification** 41. The identification function is responsible for identifying users, systems, or machines for the system engine. The primary activities of the Identification function are:

- Collect system identification configuration information from the system engine;
- Based on the configuration the identification function performs:
- Request from a user, system, or machine a logon name;
- Request from a user, system, or machine a password;

- Request from a user, system, or machine a digital certificate; and

- Request from a user, system, or machine an answer for challenge question.

- Return the above information to the system engine to continue processing the request.

3. **Digital Certificate Validation** 42. The digital certificate validation function is responsible for validating the certificate. This function can validate all kinds of certificates, whether locally in the corporate LAN or third party certificates. In addition, it can connect to the certificate server with or without encryption. The primary activities of this function are:

- Collect system digital certificate validation configuration from the system engine;

- Receive the certificate information from the system engine;

- Based on the configuration, this function performs:

- Establish a connection to the issuing certificate server with or without encryption;

- Request the certificate status from a certificate revocation list;

- Update the certificate status in the system database 49; and

- Return the certificate status information to the system engine.

4. **Authentication** 43. Authentication is the means of gaining confidence that remote customers or systems are who or what they claim to be. Reliable authentication is needed to enforce access control, establish accountability, and to achieve non-repudiation. The authentication function verifies the user's identity with the system database. The primary activities of the authentication function are:

- Collect system authentication configuration from the system engine;

- Receive the identification information from system engine;

- Verify all the identification information;

- The authentication function binds the digital certificate to customer account in the following scenarios:

- Single certificate for a single account;

- Multiple certificates for a single account; and

- Single certificate for multiple accounts.

- Return the result of the authentication process to the system engine to continue processing the request.

5. **Authorization** 44. The authorization function checks the user request and compares it with a pre-defined authorization profile. The primary activities of the authorization function are:

- Collect system authorization configuration from the system engine;

- Receive the authorization profile from the system engine;

- Check if the user request is permitted based upon the end user's authorization profile;

- Handle sending a response to the user when a disallowed request is detected; and

- Return the result of the authorization to the system engine to continue processing the request.

6. **Session Management** 45. The Web server processes each HTTP request without binding it to the previous request of the same user. This makes it stateless machine. The HTTP session management function is responsible for establishing sessions for all HTTP requests. The primary activities of the session management function are:

- Collect system session management configuration from the system engine, including:
- Session time out;
- Session clean up time for inactive sessions; and
- Enable/Disable switch.
- Receive the user session packet from the system engine;
- Group all user requests in a session;
- Update user session packet ;
- Check if the user's request derives from an active session;
- Initiate new sessions as required;
- Return the results of session management activities to the system engine to continue processing the request; and
- Terminate sessions as required.

7. **HTTP Application Dispatcher** 46. The HTTP application dispatcher function provides the user access to applications, pages, and/or services available to them based upon their authorization profile. The primary activities of this function are:

- Collect system HTTP application dispatcher configuration from the system engine, including:
  - The dispatcher HTML files location; and
  - Dispatcher links and types.
- Receive the user packet from system engine;
- Based on the user authorization profile and dispatching configuration information determine and perform:
  - The service options that are available for each specific user; and
  - Parse the services options to provide a dynamic HTML document to the user.
- Return the results of the HTTP application dispatcher activities to the system engine to continue processing the request.

8. **Logging and Non-Repudiation** 47. The logging and non-repudiation function is responsible for keeping track of every user request and its status throughout system processing. It records this data for reporting and monitoring purposes. In addition, the data it collects can be used for generating statistics about the use of the system. The primary activities of the logging and non-repudiation function are:

- Collect system logging and non-repudiation configuration from the system engine;
- Receive logging requests from the system engine;

- Register request status information from the system engine;
- Time stamp every request that travels through the system engine;
- Register the results of each request throughout system processing; and
- Save data in an encrypted database.

9. **System Administration and Maintenance** 48. The system administration and maintenance function is responsible for configuring, maintaining, managing, monitoring, and customizing the system. The primary activities of system administration and maintenance function are:

- Provide user configuration and management;
- Provide configuration and management facilities for each of the system's functions;
- Operation configuration and management; and
- Reporting and operation monitoring.

System Context Model

This section describes the external entities and events (activities) related to the invention. Fig. 5 is a block schematic diagram showing a context model according to the invention. These external entities are referenced in the context model diagram as follows:

WT-EE1: Customer;
WT-EE2: Secure HTTP / Web Server;
WT-EE3: MIS Department (MISD);
WT-EE4: Internet Application and URL;
WT-EE5: Application Logs; and
WT-EE6: Certificate Authority.

WT-EE1 – Customer

Description: Internet/Intranet/Extranet user accessing the enterprise Web-based information.

Events:

1. Customer requires access (Start a session) to any Web based application over Internet/Intranet/Extranet.

2. The system initiates customer's authentication procedures, then logs the result of the procedures.

3. Authenticated customer access the specified application, then logs all the activities of the customer on the system.

4. Customer quits the session.

WT-EE2 – Secure HTTP / Web Server

Description: Secure Web server (SHTTP Daemon).

Events:

- The server responds to customer requests;

- The system intercepts HTTP processes and initiates the authentication process based on a decision from active session manager;

- The authenticated customer is monitored by the following processes:

- Log session information process;

- Active session manager process;
- Log user request process;
- Certificate revocation process; and
- Logging user access information process.
- Then HTTP is allowed to process the customer request.

WT-EE3 – MIS Department (MISD)

Description: Enterprise management information system department.

Events:

- MISD needs to maintain (Modify, Add, Delete, (MAD)) login users information;
- System initiates MISD authentication process;
- MISD authenticates with the system;
- System displays authenticated MISD users maintenance page;
- Authenticated MISD perform the maintenance (MAD) to users login information database; and
- MISD quits session.

WT-EE4 – Internet Application and URL

Description: Web-enabled applications and/or internal Web pages.

Events:

- Customer requests access to the Internet application;
- The system initiates the authentication process including all other processes; and
- Authenticated customer gets access to the Internet application .

WT-EE5 – Application Logs

Description: Logs specific to each application.

Events:

- The system keeps logs for all activities on the secure HTTP server; and
- The system provides a set of API's to consolidate system logs with the Internet application.

WT-EE6 – Certificate Authority

Description: Enterprise local certificate issuer authority or third party certificate issuer authority.

Events:

- Customer request to access the application;
- The system initiates the authentication process by requesting user name, password, and certificate;
- The systems checks who issued the certificate (Local or Certificate Authority);

- The system checks with the certificate authority issuer on the certificate status (revoked or valid); and

- The system closes the connection with the certificate authority.

System Application Process Model

The invention provides an advanced session manager for HTTP servers to provide non-repudiation mechanism for Internet/Intranet/Extranet applications using digital IDs. The main functions of a system incorporating the invention are:

- Authenticate customers using User Name + Password + Certificate;

- Session management to provide a non-repudiation mechanism; and

- An Interface to the application logs to consolidate all logs.

System Application Processes

Fig. 6 is a data flow diagram according to the invention. The following discussion describes the application processes related to the invention. These entities are referenced in Fig. 6 as follows:

WT-01.1 – User Authentication;

WT-01.2 – Log Session Information;

WT-01.3 – Active Session Manager;

WT-01.4 – Log User Request;

WT-01.5 – Certificate Revocation;

WT-01.6 – Log User Access Information;

WT-01.7 – User Management;

WT01.8 – Control Manager;

WT-01.9 – Error Manager; and

WT-01.10 – Report Generation.

WT-01.1 – User Authentication

Description: User Authentication Process.

Preconditions:

- A person browsing the Internet asks for access to the Internet application;
- A company MIS department staff member require access to the users maintenance screen; and
- A secure communication link between the customer browser and the HTTP/Web server.

Process:

Once a secure session is in place, the process of verification includes:

- A browser asks for access to the Internet application;
- If the person is in the active session then:
  - Calculate time interval between the last two requests (Idle Time);

- If the idle time exceeds the time out for session then:

- Move the session record from the active session manager to the session log;

- The customer is asked to submit User name + Password + Digital Certificate to verify their access (STEP 4);

- Log (User-Name, Start-Time, Certificate Serial Num, Last-Time, and IP-Num) in the Active session manager;

- Log (User-Name, Start-Time, Certificate Serial Num, Last-Time, URL, and IP-Num) in the User Request log;

- Log (User-Name, Start-Time, Certificate Serial Num, Last-Time, Message, and IP-Num) in the User Access Information log; and

- Access is permitted.

• If the person is not in the active session then:

- The customer is asked to submit User name + Password + Digital Certificate to verify their access (STEP 4);

• If User name and Password found in the Users Information database then:

- If Certificate is verified through Certificate Revocation process then:

- Log (User-Name, Start-Time, Certificate Serial Num, Last-Time, and IP-Num) in the Active session manager;

- Log (User-Name, Start-Time, Certificate Serial Num, Last-Time, URL, and IP-Num) in the User Request log;

- Log (User-Name, Start-Time, Certificate Serial Num, Last-Time, URL, and IP-Num) in the User Access Information log; and

- Access is permitted.

- If User name and Password is not found in the users information database then:

- Log this information in the users access log database; and

- Deny the service.

Post Conditions:

- Person has been authenticated to be an Internet application subscriber; and

- Person has been notified he/she is not a current Internet application subscriber.

WT-01.2 – Log Session Information

Descriptions: Process to log all user sessions on the secure HTTP server.

Preconditions: User request after idle time.

Process: Moves from active session manager log to session log .

Post Conditions: User must reauthenticate.

WT-01.3 – Active Session Manager

Descriptions: Process to manage all active sessions on the secure HTTP server.

Preconditions:

- User request access to the Internet application; and
- User authentication information.

Process:

If Active user then:

- Update active log;

- Log user request manager;

If in-active user then:

User Authentication;

If request > Idle time then:

Log user request manger;

Log user access manager;

Log session information manager; and

User Authentication.

Post Conditions: Permit user to access the Internet application.

WT-01.4 – Log User Request

Description: Process to log all user requests to the secure HTTP server.

Preconditions:

- User authentication information; and
- Uniform Resource Indicator (URI).

Process: Log URI for all requests to the secure HTTP/Web Server.

Post Conditions:

WT-01.5 – Certificate Revocation

Description: Process to check the revocation status of the submitted user certificates to the secure HTTP server.

Preconditions: User certificate.

Process:

Decode certificate;

Extract serial number, issuer organization, and revocation URL;

If revocation URL exists then:

- Create a connection to URL (Secure or Not);

- Send certificate serial number;

- Receive status;

- If Certificate is revoked then:

- Deny access;

- Permit access;

Check the certificate revocation database.

Post Conditions:

1. Return certificate status; and

2. Log user access log.

WT-01.6 – Log User Access Information

Description: Process to log access information of all users.

Preconditions: User Authentication Information.

Process: Log a message that reflects the status of authentication to the access log.

Post Conditions:

WT-01.7 – User Management

Description: Process responsible for user management operations: view, modify, add, delete (VMAD).

Preconditions: MISD has been authenticated and requires to maintain the users database.

Events:

1. Obtains the users list from users database; and

2. The process also lets MISD select a user and one of the following operations:

- Add
- View
- Modify
- Delete

3. MISD maintains the users database options:

For each of the selected users do:

Case operation is:

Add:

Process displays a form to collect the information to add a new user:

- User Name;
- Password;
- Certificate Serial Number;
- Certificate Issuer Organization;
- Status; and
- Control.

View:

Process displays the current user information.

Modify:

Process displays the current user information and lets MISD modify the information.

Delete:

Process displays the current user information and asks MISD to confirm the delete process;

MISD finishes users database maintenance and quits;

The process records this transaction in:

Session Log;
User Request Log;
Activities Log; and
User Access Log.

Post Conditions:

1. MISD has finished maintaining the users database;

2. MISD has requested to quit users options maintenance process.

WT-01.8 – Control Manager

Description: Process to control access of users requests based on predefined configuration.

Preconditions:

1. User authentication information;

2. User request information.

Process: Check control information database for access control on specified information.

Post Conditions: Allowed/Denied access based on process.

WT-01.9 – Error Manager

Description: Process that generates and logs error messages for all system processes.

Preconditions:

1. An error occurred in any system processes;

2. Any user authentication information known when error occurred; and

3. The process responsible for the error.

Process: Log error to error log database based on information obtained from calling process.

Post Conditions: Abort user request.

WT-01.10 – Report Generator

Description: Process for generating daily encrypted report from system logs.

Preconditions: Lock system database.

Process:

Dump each database table in a temporary file;

Formulate a report per table; and

Encrypt each report.

Post Conditions:

1. Clear log tables;

2. Log report process; and

3. Unlock the database.

System Application Data Model

This model describes the data structures that are used internally for the system to support system services and functions.

The model maintains data on:

1. User login information
   - Web Site Administrator
   - MIS Department (MIS)
   - Customers.

2. Certificate revocation information.

3. Active sessions on the Internet application.

4. Session log on the Internet application.

5. Access log for the Internet application.

6. Request log for the Internet application.

7. Users access control information.

8. System internal processes error log.

Application Data Stores

The following discussion describes the data stores and related events used with the system, referenced in Fig. 6 as:

- WT-DS01: Session Log;
- WT-DS02: User Request Log;
- WT-DS03: Activities Log;
- WT-DS04: User Access Log;
- WT-DS05: Users Information;
- WT-DS06: Certificate Revocation Information;
- WT-DS07: Control Information; and
- WT-DS08: Error Log.

WT-DS01 – Session Log

Description: Database table that logs all sessions on the secure HTTP server

Data Fields:

- Reference Num
- User Name
- Certificate Serial Num
- Certificate Issuer Organization
- Start Time
- End Time
- IP Num

WT-DS02 – User Request Log

Description: Database table that logs all users requests on the secure HTTP server.

Data Fields:

- Reference Num
- User Name
- Certificate Serial Num
- Certificate Issuer Organization
- Start/Finish Time
- Star/Finish Status
- URI
- IP Num

WT-DS03 – Activities Log

Description: Database table/file containing log data of all the activities on the secure HTTP server with user.

Data Fields:

- User Name
- Start Time
- Certificate Serial Num
- Certificate Issuer Organization
- Last Time
- IP Num

WT-DS04 – User Access Log

Description: Logging all user access to the system.

Data Fields:

- Reference Num
- User Name
- Certificate Serial Num
- Certificate Issuer Organization
- Start Time
- Message
- IP Num

WT-DS05 – User Information

Description: Database table that contains users login information.

Data Fields:

- User Name
- Password
- Certificate Serial Num
- Certificate Issuer Organization
- Status
- Control

WT-DS06 – Certificate Revocation Information

Description: Database table that contains all the revoked certificates information.

Data Fields:

- Certificate Serial Num
- Certificate Issuer Organization
- Status

WT-DS07 – Control Information

Description: Database table that contain access control information for users.

Data Fields:

- User Name
- Certificate Serial Num
- Certificate Issuer Organization
- File Name
- URI
- Access Limit Num
- Current Access Count Num
- Type

WT-DS08 – Error Log

Description: Database table that contains error messages.

Data Fields:

- Reference Num
- User Name
- Certificate Serial Num
- Certificate Issuer Organization
- Current Time

- Message
- Process ID
- URI
- IP Num

Main Modules

Fig. 7 is a block schematic diagram showing an Internet billing application context model according to the invention, and Fig. 8 is a block schematic diagram showing an Internet billing application process and data model according to the invention. The following discussion describes the main modules of an example (XYZ) Internet billing application. These modules are referenced in Figs. 7 and 8 as follows:

DFD: SYSTEM (SECURE APP MANAGER)
DFD: CUSTOMER (CUSTOMER ASSISTANCE ENGINE)
DFD: ADMINISTRA (STAFF ASSISTANT ENGINE).

SYSTEM (SECURE APP MANAGER)

Description:

The secure application manager administers the users security access profiles and it is the only mechanism with which the user is allowed to access the application. This is a must for all users of the Internet and Intranet applications (customers and staff).

The secure application manager is responsible for:

1. User authentication and access control for all IBA users (customers and staff), based on:

- DID;

- Login and password; and

- Challenge question mechanism (optional).

2. Continuous authentication of user requests (based on DID).

3. Session Management .

4. Logging user activity (for statistics and non-repudiation).

5. Shows the modules of the application the user has the right to access and transfer the control to the user selected module responsible to handle his/her request, passing to it (at least) the customer IDs and DID (if available) information. This information is used by the module (see CUSTOMER and ADMINISTRA).

6. It contains an administration application to:

- Add/modify/delete information about user authentication information and access permissions;

- Generate access reports for security audit, statistics and non-repudiation;

- Modify access roles to the application based on business and data security roles.

7. Handling communication encryption (SSL).

8. Handling memory encryption to QTEL applications in the framework of Internet billing and administration of the Internet system.

9. Insuring revocation status for all DID access (internet or intranet Based).

10. For new user, the app manager should Automatically bind a user DID (when applicable) to the customer entry in the customer database (NETCUSTDB).

The app manager must have access to internal user access profile (database or permission files) to determine application access by the user. The application manager also must have the capabilities to allow users access, after authenticating them, to HTML files, database and/or Java-based applications.

XYZ Telecommunications Internet Billing Functionality

The following discussion explains XYZ telecommunications Internet billing functionality. Fig. 9 is a block schematic diagram showing functional decomposition of an Internet billing application according to the invention, and Fig. 10 is a block schematic diagram showing functional decomposition of an Internet bill payment and presentment application according to the invention. Fig. 9 explains the functional breakdown of the XYZ Internet Billing Application where the invention serves as the security mechanism. This figure breaks down the functions by role as they exist in the organization's business structure. Each block contains a set of functions (forms, programs, etc.) that are available to users permitted access to that portion of XYZs IBA. Under Administration, the Internet Billing Administration Department has access and authority to manage the security and audit facilities that are under the control of the invention. Figure 10 is a detail of the Administration side of Fig. 9 and includes the services available within each block. The invention can be managed through the "Security System Management" block under Internet Billing Administration. All changes made to the Invention's configuration will be reflected throughout the system and affect all customers and administrators.

XYZ Internet billing administration department components (functions):

Security system management components:

These functional components are used by the administration department (ADMIN) staff members to manage, monitor and administer the system (Secure Application Manager) and modify parameter values for the security mechanisms. The application components access the business rules database for needed parameters. The components register all user events and local database access status to the log file.

Fig. 11 is a block schematic diagram of a network segmentation model according to the invention. This figure shows a physical network layout as might be encountered in a typical installation for the invention. In this case, we use XYZ Corporation Internet Billing Application. The IBA Server is the server that hosts the invention and the IBA. The IBA may be linked to other machines from which it gathers or manipulates data. All the application components which are accessed through the Web Server being controlled and protected by the invention will benefit from the security, access and audit protections that it provides.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

1. A non-repudiation apparatus for electronic transactions performed over an electronic network, comprising:

at least one server;

at least one application;

a link between said server and said application;

means within said link for providing an audit trail to effect non-repudiation; and

means within said link for controlling a session between said server and said application;

wherein each and every request made via said electronic network pursuant to said electronic transaction is correlated to a user.

2. The apparatus of Claim 1, wherein said link manages and coordinates all traffic through said server and imposes security and access rules which are associated with each user and each uniform resource indicator.

3. The apparatus of Claim 1 wherein said link connects said server and said application to form a continuous and unbroken, reconcilable and auditable audit trail that establishes accountability of system users.

4. The apparatus of Claim 1, said electronic network comprising the Internet; said link further comprising:

a single sign-on mechanism for all Internet applications accessible through said server.

5. The apparatus of Claim 1, said link further comprising:

a digital signature mechanism for identifying a person requesting services from a system and for tracking said person's actions throughout their session with said system.

6. The apparatus of Claim 1, said link further comprising:

an authentication mechanism for enforcing authentication for each and every action requested from each user, said authentication mechanism performing authentication checks for both local and third party digital ID issuers to confirm validity and establish identity, said authentication mechanism binding digital certificates and passwords together pursuant to an authorization sequence, wherein a second layer of authentication is optionally provided to enforce challenge questions if a user's security assessment requires extremely strict measures.

7. The apparatus of Claim 1, said link further comprising:

an access control mechanism for controlling information and applications which individuals and groups are permitted to access, wherein access control is performed continuously for every request made to a system, and wherein access rights are set by any of time, frequency, and number of visits to a specific location, and a sequence in which information is requested.

8. The apparatus of Claim 1, said link further comprising:

a data integrity mechanism for ensuring that information sent and received is unaltered, wherein said data integrity mechanism asserts data integrity functions by use of cryptography.

9. The apparatus of Claim 1, said link further comprising:

a non-repudiation mechanism for enabling clear reports that establish a complete and unbroken audit trail.

10. The apparatus of Claim 1, said link further comprising:

a monitoring and alarms mechanism for permitting alarms to be configured should illegal or improper activities be discovered, wherein alarms can be set to perform any of cutting communications, suspending access rights, and paging security personnel, and wherein records of security breeches are maintained.

11. The apparatus of Claim 1,wherein said link manages access control and flow control by any of individual, group, application, file, page, date, time, or exception handling.

12. The apparatus of Claim 1, wherein said link may be installed at both ends of an Internet transmission to establish a virtual private network in which security is executed at said application itself.

13. An apparatus for providing secure HTTP protocol applications, comprising:

at least one server;

at least one application; and

a link between said server and said application for establishing presentation and session control for said HTTP protocol to provide identification, authentication, authorization, access control, and non-repudiation capabilities for application users.

14. The apparatus of Claim 13, said link comprising:

a client identification module;

a digital certificate validation module;

a data encryption module;

a client authentication module;

a client authorization module;

a session management module;

an HTTP application dispatching module;

a logging module for establishing non-repudiation;

an exception handling module; and

a system administration and maintenance module.

15. A system for providing secure HTTP protocol applications, comprising:

a system situated at a service provider organization in communication with a certificate authority trusted by said service provider organization to issue digital signatures to end users to allow trusted communication with said service provider organization system, said service provider system also in communication with an end user

system that interacts with said service provider organization using a secure communication channel via a public network; and

a link between said service provider organization system and said public network which identifies, authenticates, authorizes, and establishes user sessions, controls application flow, and tracks end users and/or end user requests throughout a communication session.

16. The system of Claim 15, said service provider organization further comprising:

policies and procedures that govern the interaction of people with a network to ensure security and compliance with established business processes;

a server that responds to incoming requests and initiates a secure connection using cryptographic mechanisms; and

an HTTP application for attending to end user and/or entity requests for services and/or products.

17. A security architecture for an HTTP application, comprising:

a system in which said HTTP application is passed parameters based upon individually established configurations, wherein all parameters are enabled, disabled, and customized per application, per system function, per user, and per administrator, said system comprising:

a system engine for controlling system operations which are based on administration configurations;

an identification module for identifying users, systems, or machines for said system engine;

a digital certificate validation module responsible for validating a digital certificate;

an authentication module for enforcing access control, establishing accountability, and providing non-repudiation;

authorization module for checking a user request and comparing said user request with a pre-defined authorization profile;

a session management module for establishing sessions for all requests;

an HTTP application dispatcher module for providing a user with access to applications, pages, and/or services available to said user based upon said user's authorization profile;

a logging and non-repudiation module for keeping track of every user request and its status throughout system processing; and

a system administration and maintenance module for configuring, maintaining, managing, monitoring, and customizing said system.

18. The architecture of Claim 17, wherein said system engine reads system configuration from a database at system startup; handles client requests; encrypts data in both said database and in a system memory; reserves, manages, and protects memory; instructs each function how to perform based upon system configuration; invokes functions based on user request status; constructs and manages current user packets; provides a log-out page; provides a user change password facility; send parameters and format to said HTTP application; and constructs application parameters.

19. The architecture of Claim 17, wherein said identification module collects system identification configuration information from said system engine and based on a particular system configuration said identification module handles:

requests from a user, system, or machine a logon name;

requests from a user, system, or machine a password;

requests from a user, system, or machine a digital certificate; and

requests from a user, system, or machine an answer for challenge question,

wherein said identification module returns results of such requests to said system engine to continue processing a request.

20. The architecture of Claim 17, wherein said digital certificate validation module validates all kinds of certificates, whether locally in a corporate LAN or third party certificates, wherein said digital certificate validation module:

collects a system digital certificate validation configuration from said system engine;

receives certificate information from said system engine; and

based on system configuration:

establishes a connection to an issuing certificate server with or without encryption;

requests certificate status from a certificate revocation list;

update certificate status in a system database; and

return said certificate status information to said system engine.

21. The architecture of Claim 17, wherein said authentication module verifies a user's identity with a system database, and wherein said authentication module:

collects system authentication configuration from said system engine;

receives identification information from said system engine; and

verifies said identification information;

binds a digital certificate to a customer account in any of the following:

a single certificate for a single account;

multiple certificates for a single account; and

a single certificate for multiple accounts;

returns a result of an authentication process to said system engine to continue processing said request.

22. The architecture of Claim 17, wherein said authorization module:

collects system authorization configuration from said system engine;

receives said authorization profile from said system engine;

checks if said user request is permitted based upon an end user's authorization profile;

handles sending a response to said user when a disallowed request is detected; and

returns a result of said authorization to said system engine to continue processing said request.

23. The architecture of Claim 17, wherein said session management module:

collects system session management configuration from said system engine;

receives a user session packet from said system engine;

groups all user requests in a session;

updates a user session packet;

checks if a user's request derives from an active session;

initiates new sessions as required;

returns results of session management activities to said system engine to continue processing the request; and

terminates sessions as required.

24. The architecture of Claim 17, wherein said application dispatcher module:

collects an application dispatcher configuration from said system engine;

receives a user packet from said system engine;

based on the user authorization profile and dispatching configuration information, determines and performs:

service options that are available for each specific user; and

parses said service options to provide a dynamic document to said user;

returns results of said application dispatcher activities to said system engine to continue processing said request.

25. The architecture of Claim 17, wherein said logging and non-repudiation module records data for reporting and monitoring purposes, wherein said logging and non-repudiation module:

collects system logging and non-repudiation configuration from said system engine;

receives logging requests from said system engine;

registers request status information from said system engine;

time stamps every request that travels through said system engine;

registers results of each request throughout system processing; and

saves data in an optionally encrypted database.

26. The architecture of Claim 17, wherein said system administration and maintenance module:

provides user configuration and management; and

provides configuration and management facilities for each of said system's functions.

27. In a system in which an HTTP application is passed parameters based upon individually established configurations, wherein all parameters are enabled, disabled, and customized per application, per system function, per user, and per administrator, a security method for said HTTP application, comprising the steps of:

controlling system operations which are based on administration configurations;

identifying users, systems, or machines for a system engine;

validating a digital certificate;

enforcing access control, establishing accountability, and providing non-repudiation;

checking a user request and comparing said user request with a pre-defined authorization profile;

establishing sessions for all requests;

providing a user with access to applications, pages, and/or services available to said user based upon said user's authorization profile;

keeping track of every user request and its status throughout system processing; and

configuring, maintaining, managing, monitoring, and customizing said system.

28. A method for providing secure HTTP protocol applications, comprising the steps of:

providing a system situated at a service provider organization in communication with a certificate authority trusted by said service provider organization to issue digital signatures to end users to allow trusted communication with said service provider organization system, said service provider system also in communication with an end user system that interacts with said service provider organization using a secure communication channel via a public network; and

providing a link between said service provider organization system and said public network which identifies, authenticates, authorizes, and establishes user sessions, controls application flow, and tracks end users and/or end user requests throughout a communication session.

29. A method for providing secure HTTP protocol applications, comprising the steps of:

providing at least one server;

providing at least one application; and

providing a link between said server and said application for establishing presentation and session control for said HTTP protocol to provide identification, authentication, authorization, access control, and non-repudiation capabilities for application users.

30. A non-repudiation method for electronic transactions performed over an electronic network, comprising the steps of:

providing at least one server;

providing at least one application;

providing a link between said server and said application;

providing means within said link for providing an audit trail to effect non-repudiation; and

providing means within said link for controlling a session between said server and said application;

wherein each and every request made via said electronic network pursuant to said electronic transaction is correlated to a user.

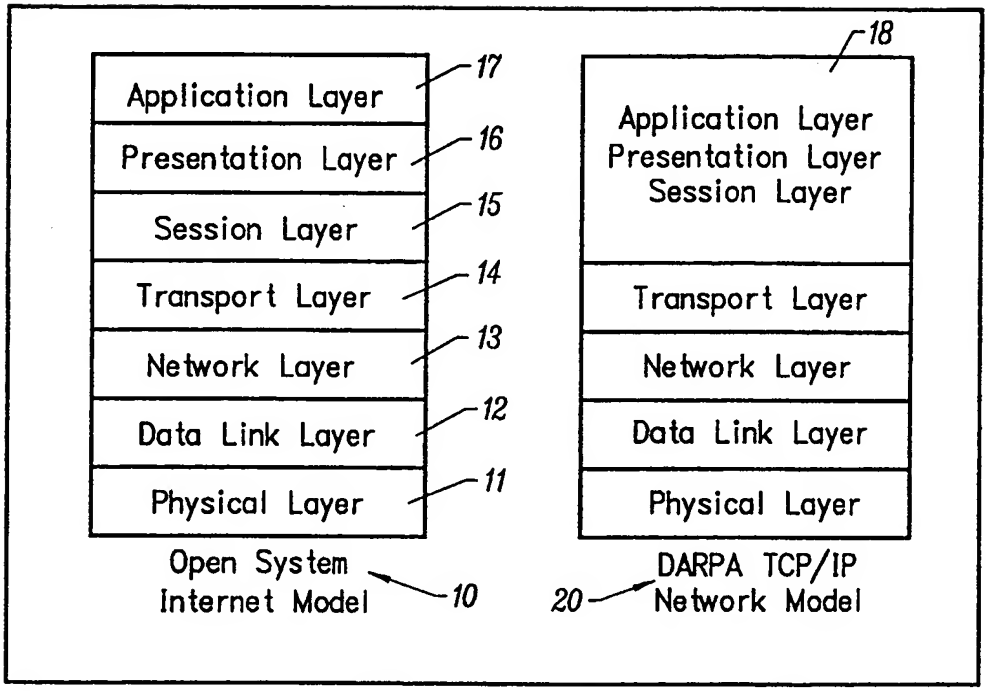


FIG. 1
PRIOR ART

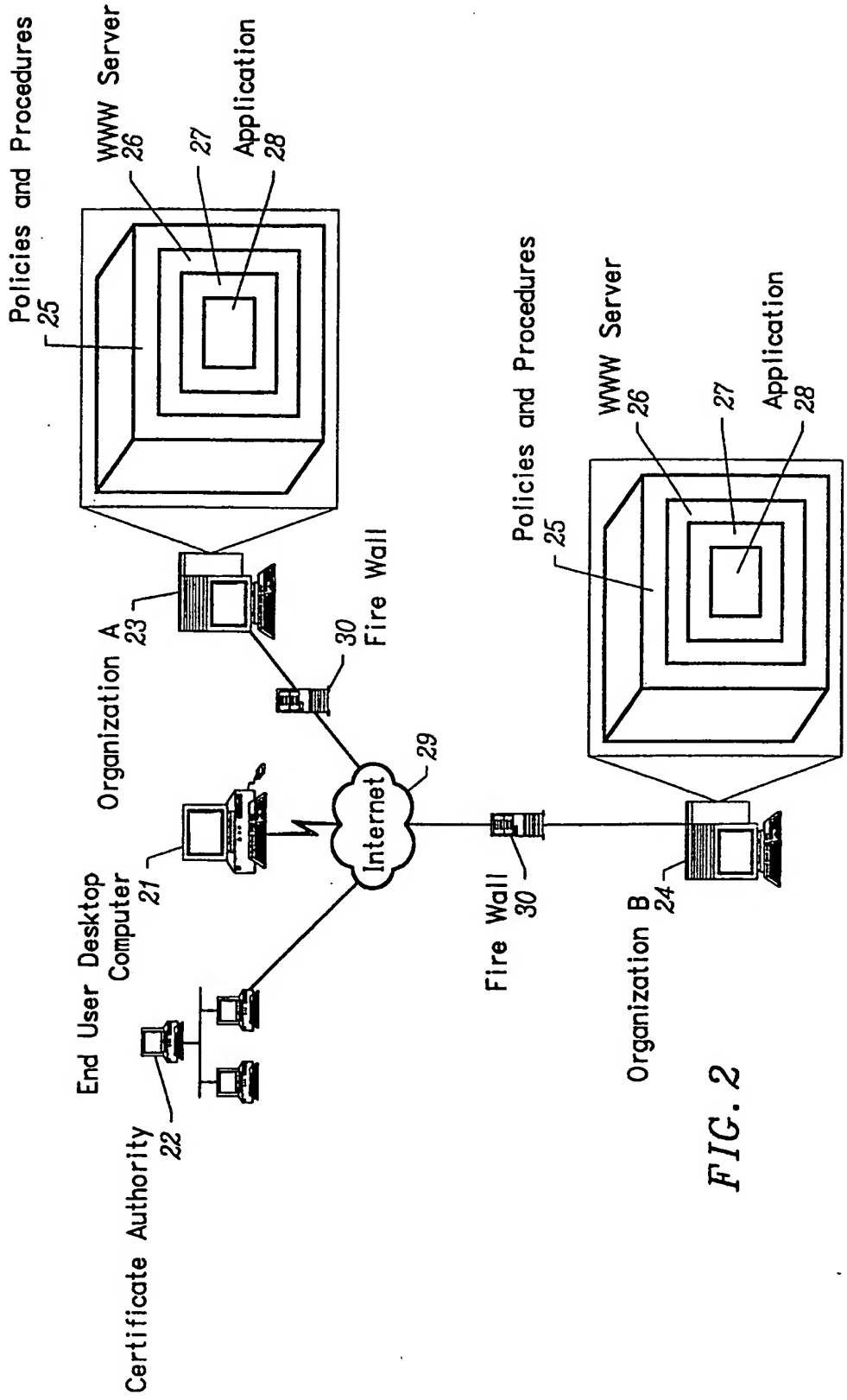

Policies and Procedures
25
WWW Server
26
27
Application
28
Organization A
23
30
Fire Wall
29
Internet
End User Desktop Computer
21
Certificate Authority
22
Fire Wall
30
Policies and Procedures
25
WWW Server
26
27
Application
28
Organization B
24

FIG. 2

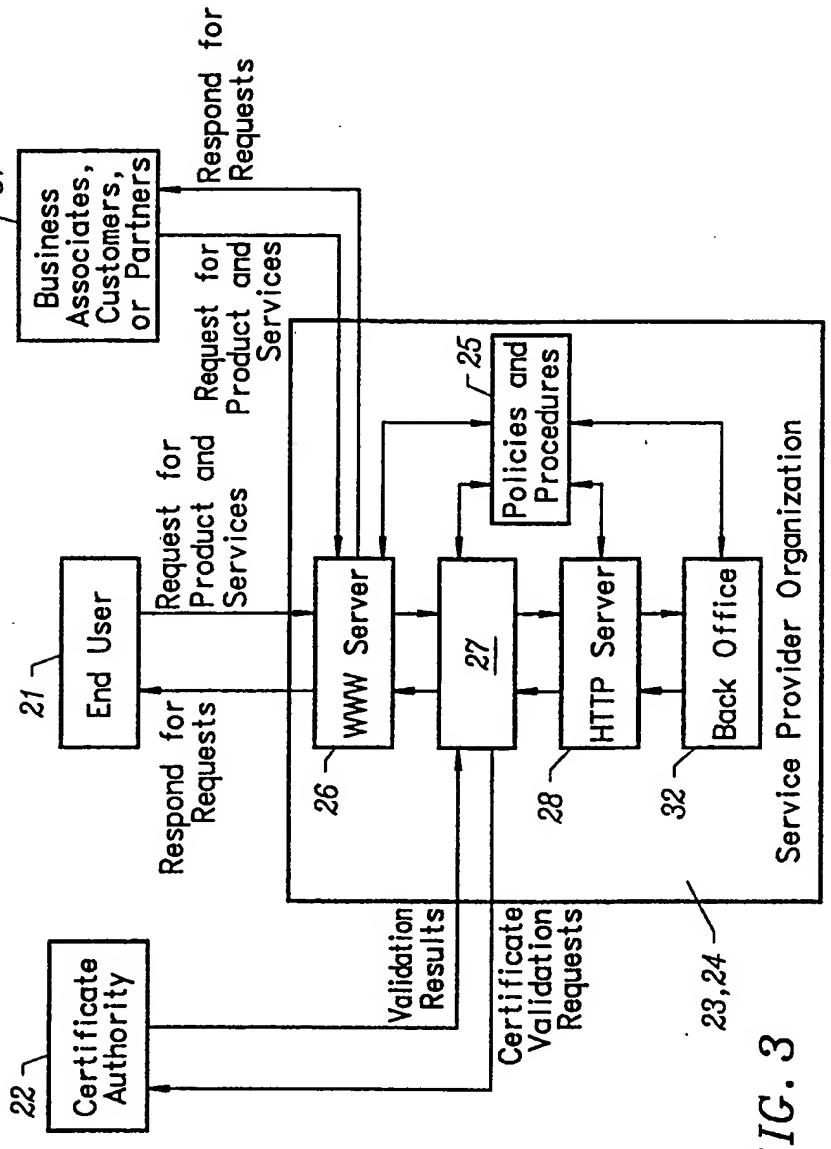

Business Associates, Customers, or Partners
31
Respond for Requests
Request for Product and Services
Policies and Procedures
25
End User
21
Request for Product and Services
Respond for Requests
WWW Server
26
27
HTTP Server
28
Back Office
32
Service Provider Organization
23,24
Validation Results
Certificate Validation Requests
Certificate Authority
22

FIG. 3

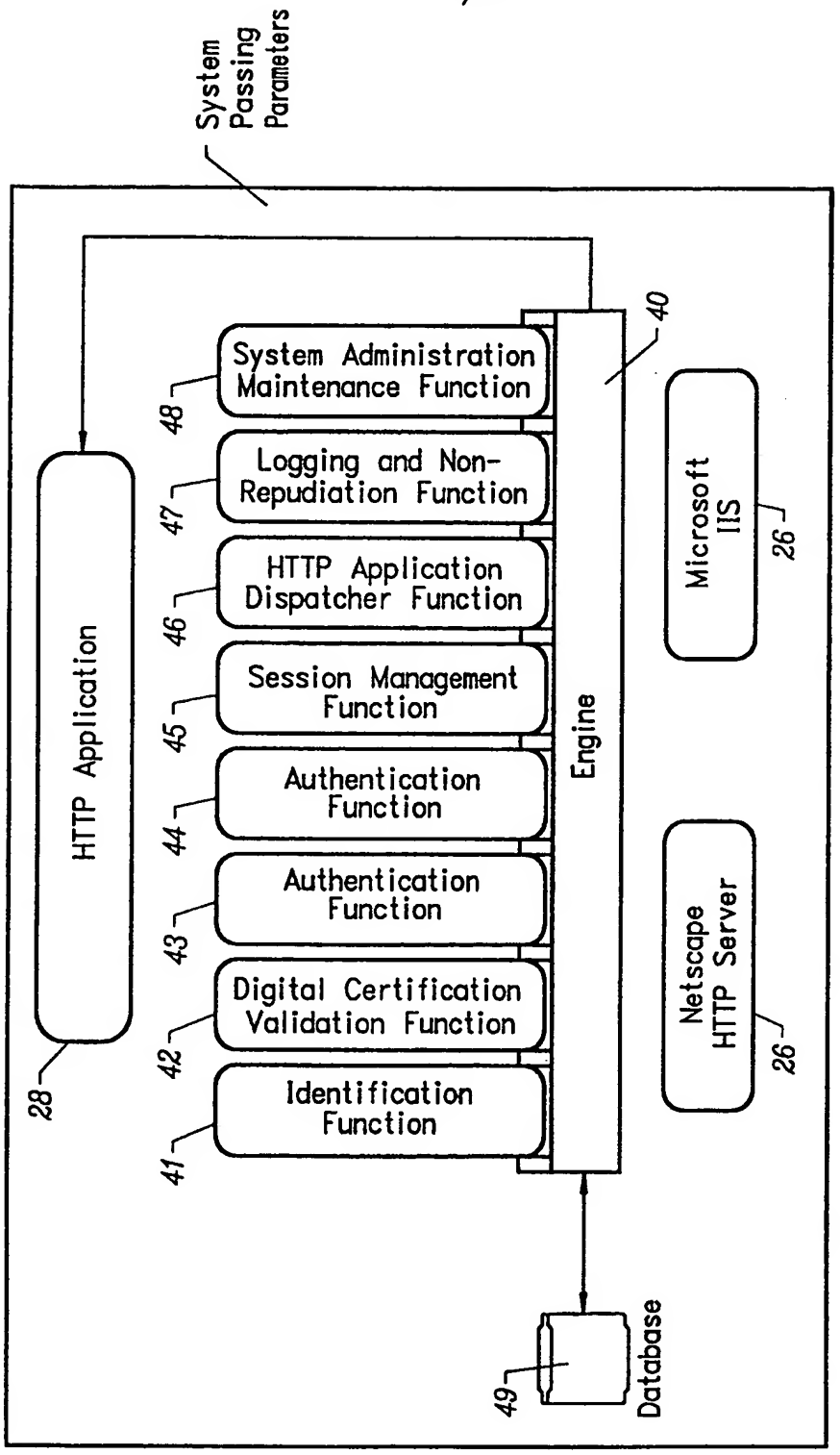

System Passing Parameters
HTTP Application
28
System Administration Maintenance Function
48
Logging and Non-Repudiation Function
47
HTTP Application Dispatcher Function
46
Session Management Function
45
Authentication Function
44
Authentication Function
43
Digital Certification Validation Function
42
Identification Function
41
Engine
40
Microsoft IIS
26
Netscape HTTP Server
26
Database
49

FIG. 4

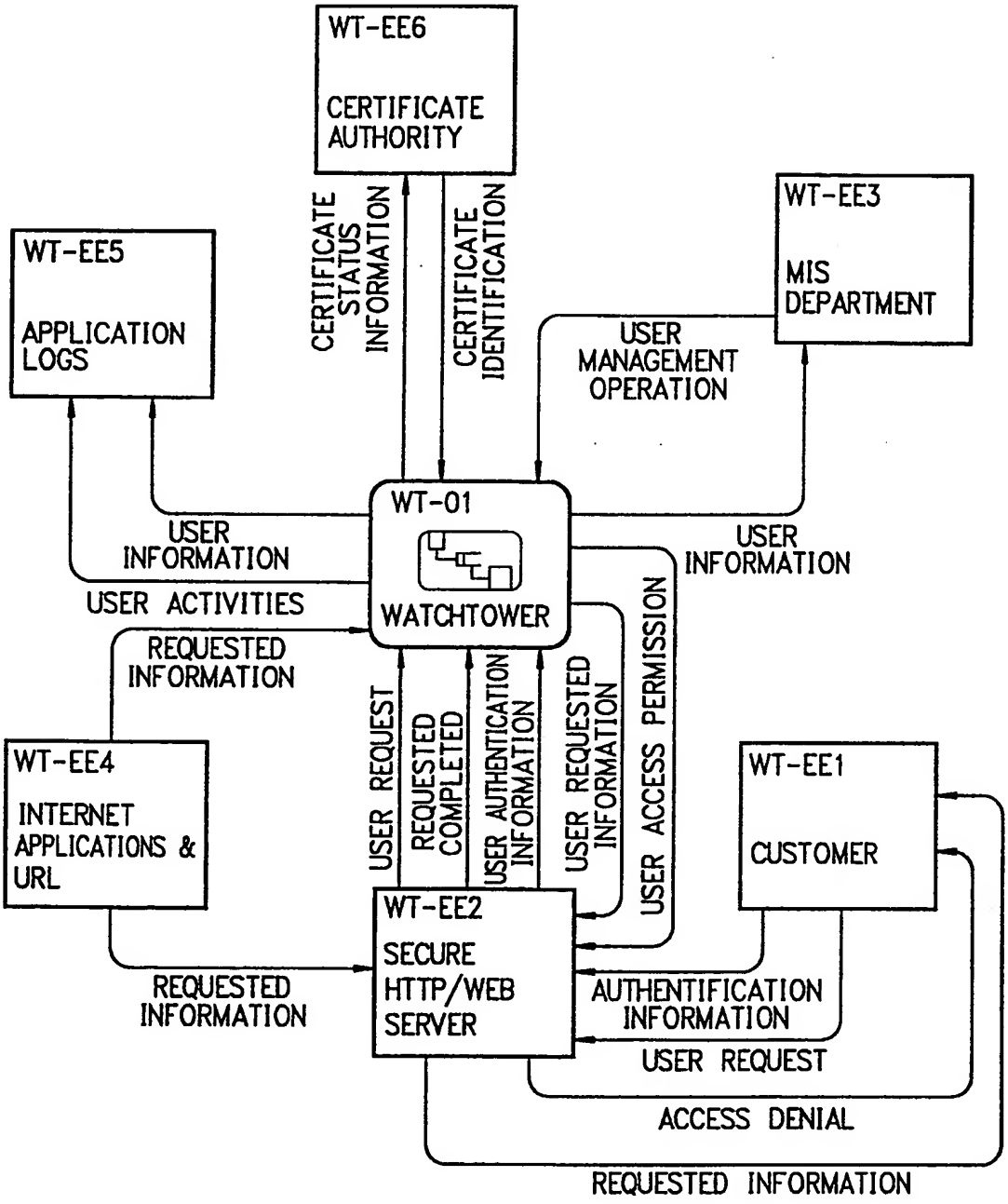

WT-EE6
CERTIFICATE AUTHORITY
CERTIFICATE STATUS INFORMATION
CERTIFICATE IDENTIFICATION
WT-EE3
MIS DEPARTMENT
WT-EE5
APPLICATION LOGS
USER MANAGEMENT OPERATION
WT-01
WATCHTOWER
USER INFORMATION
USER ACTIVITIES
USER INFORMATION
REQUESTED INFORMATION
USER REQUEST
REQUESTED COMPLETED
USER AUTHENTICATION INFORMATION
USER REQUESTED INFORMATION
USER ACCESS PERMISSION
WT-EE4
INTERNET APPLICATIONS & URL
WT-EE1
CUSTOMER
WT-EE2
SECURE HTTP/WEB SERVER
REQUESTED INFORMATION
AUTHENTIFICATION INFORMATION
USER REQUEST
ACCESS DENIAL
REQUESTED INFORMATION

FIG. 5

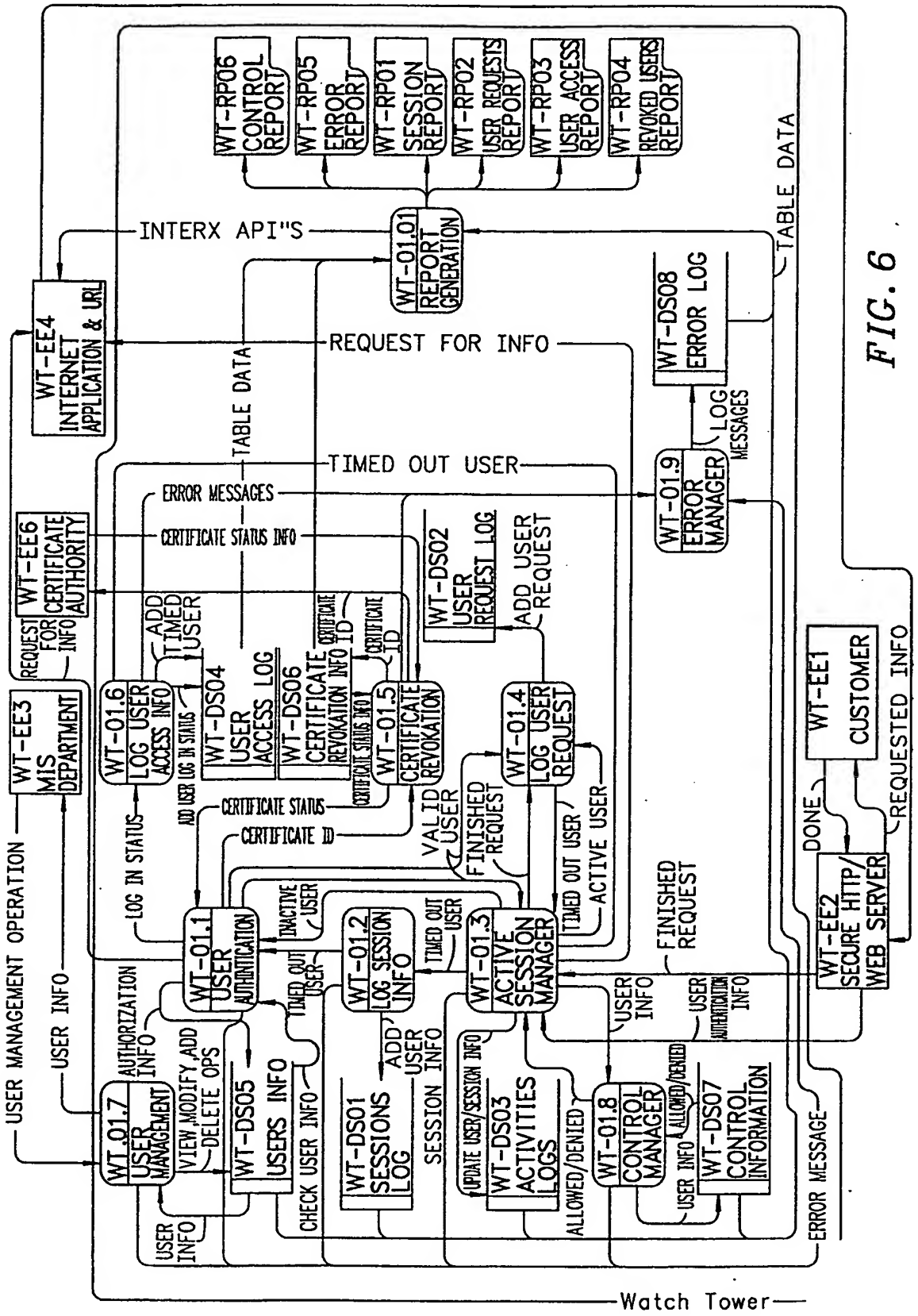

WT-RP06 CONTROL REPORT
WT-RP05 ERROR REPORT
WT-RP01 SESSION REPORT
WT-RP02 USER REQUESTS REPORT
WT-RP03 USER ACCESS REPORT
WT-RP04 REVOKED USERS REPORT
INTERX API"S
WT-01.01 REPORT GENERATION
TABLE DATA
WT-EE4 INTERNET APPLICATION & URL
REQUEST FOR INFO
WT-DS08 ERROR LOG
LOG MESSAGES
TIMED OUT USER
ERROR MESSAGES
WT-01.9 ERROR MANAGER
CERTIFICATE STATUS INFO
WT-EE6 CERTIFICATE AUTHORITY
REQUEST FOR INFO
ADD TIMED USER
WT-DS02 USER REQUEST LOG
ADD USER REQUEST
WT-01.6 LOG USER ACCESS INFO
WT-DS04 USER ACCESS LOG
WT-DS06 CERTIFICATE REVOKATION INFO
WT-01.5 CERTIFICATE REVOKATION
WT-01.4 LOG USER REQUEST
WT-EE3 MIS DEPARTMENT
WT-EE1 CUSTOMER
DONE
REQUESTED INFO
USER MANAGEMENT OPERATION
USER INFO
LOG IN STATUS
CERTIFICATE STATUS
CERTIFICATE ID
VALID USER
FINISHED REQUEST
TIMED OUT USER
ACTIVE USER
WT-01.1 USER AUTHENTICATION
WT-01.2 LOG SESSION INFO
WT-01.3 ACTIVE SESSION MANAGER
WT-EE2 SECURE HTTP/ WEB SERVER
FINISHED REQUEST
INACTIVE USER
TIMED OUT USER
AUTHORIZATION INFO
USER INFO
USER AUTHENTICATION INFO
WT-01.7 USER MANAGEMENT
VIEW, MODIFY, ADD DELETE OPS
WT-DS05 USERS INFO
CHECK USER INFO
WT-DS01 SESSIONS LOG
ADD USER SESSION INFO
UPDATE USER/SESSION INFO
WT-DS03 ACTIVITIES LOGS
ALLOWED/DENIED
WT-01.8 CONTROL MANAGER
USER INFO
ALLOWED/DENIED
WT-DS07 CONTROL INFORMATION
USER INFO
ERROR MESSAGE
Watch Tower

FIG. 6

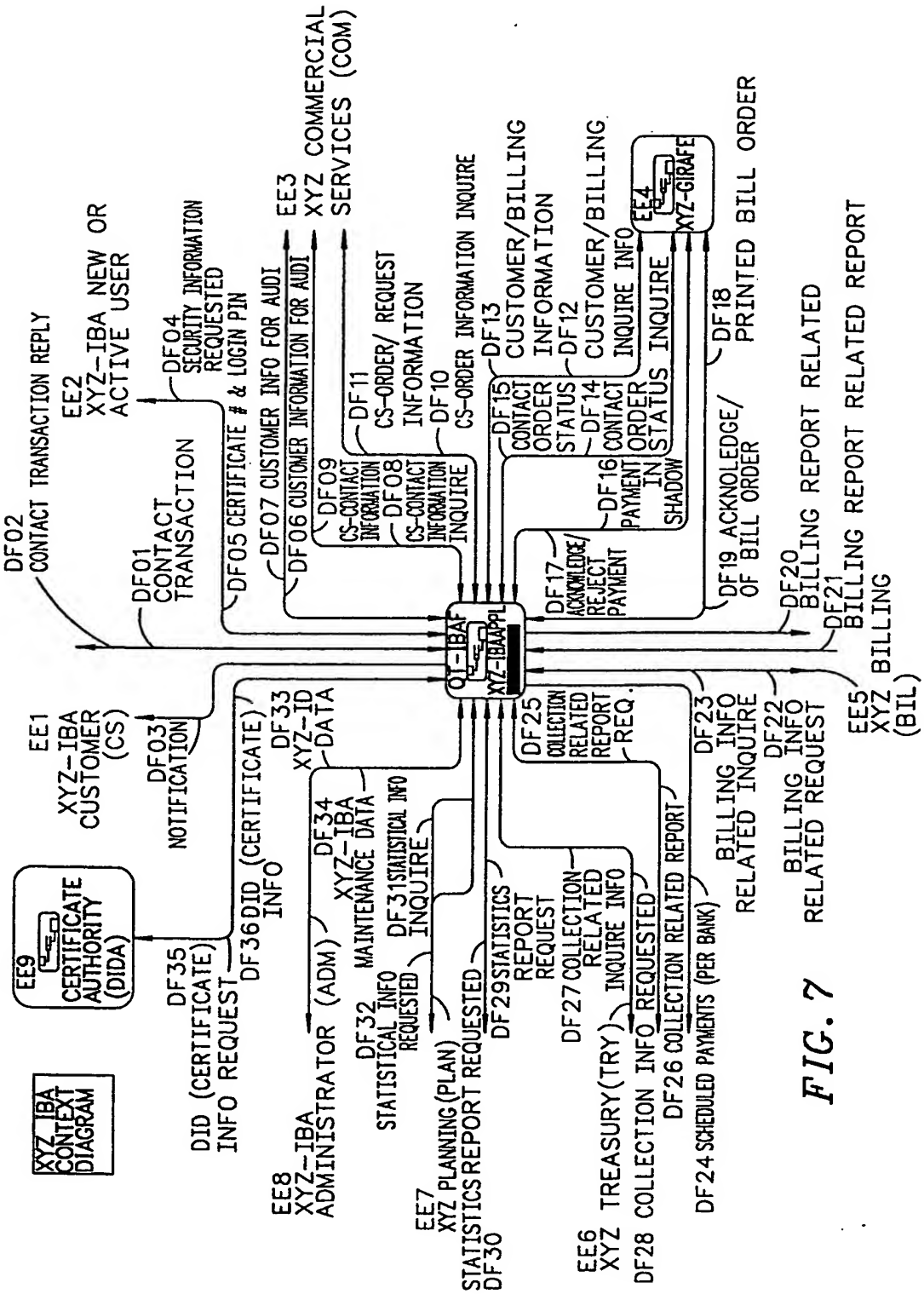

XYZ IBA CONTEXT DIAGRAM
EE9 CERTIFICATE AUTHORITY (DIDA)
EE1 XYZ-IBA CUSTOMER (CS)
EE2 XYZ-IBA NEW OR ACTIVE USER
EE3 XYZ COMMERCIAL SERVICES (COM)
EE4 XYZ-GIRAFE
EE5 XYZ BILLING (BIL)
EE6 XYZ TREASURY(TRY)
EE7 XYZ PLANNING(PLAN)
EE8 XYZ-IBA ADMINISTRATOR (ADM)
DF01 CONTACT TRANSACTION
DF02 CONTACT TRANSACTION REPLY
DF03 NOTIFICATION
DF04 SECURITY INFORMATION REQUESTED
DF05 CERTIFICATE # & LOGIN PIN
DF06 CUSTOMER INFORMATION FOR AUDI
DF07 CUSTOMER INFO FOR AUDI
DF08 CS-CONTACT INFORMATION INQUIRE
DF09 CS-CONTACT INFORMATION
DF10 CS-ORDER INFORMATION INQUIRE
DF11 CS-ORDER/ REQUEST INFORMATION
DF12 CUSTOMER/BILLING INQUIRE INFO
DF13 CUSTOMER/BILLING INFORMATION
DF14 CONTACT ORDER STATUS
DF15 CONTACT ORDER STATUS
DF16 PAYMENT IN SHADOW
DF17 ACKNOLEDGE/ REJECT PAYMENT
DF18 PRINTED BILL ORDER
DF19 ACKNOLEDGE/ OF BILL ORDER
DF20 BILLING REPORT RELATED
DF21 BILLING REPORT RELATED REPORT
DF22 BILLING INFO RELATED REQUEST
DF23 BILLING INFO RELATED INQUIRE
DF24 SCHEDULED PAYMENTS (PER BANK)
DF25 COLLECTION RELATED REPORT REQ.
DF26 COLLECTION RELATED REPORT
DF27 COLLECTION RELATED INQUIRE INFO
DF28 COLLECTION INFO REQUESTED
DF29 STATISTICS REPORT REQUEST
DF30 STATISTICS REPORT REQUESTED
DF31 STATISTICAL INFO INQUIRE
DF32 STATISTICAL INFO REQUESTED
DF33 XYZ-ID DATA
DF34 XYZ-IBA MAINTENANCE DATA
DF35 DID (CERTIFICATE) INFO REQUEST
DF36 DID (CERTIFICATE) INFO
QI-IBA
XYZ-IBAAPPL

FIG. 7

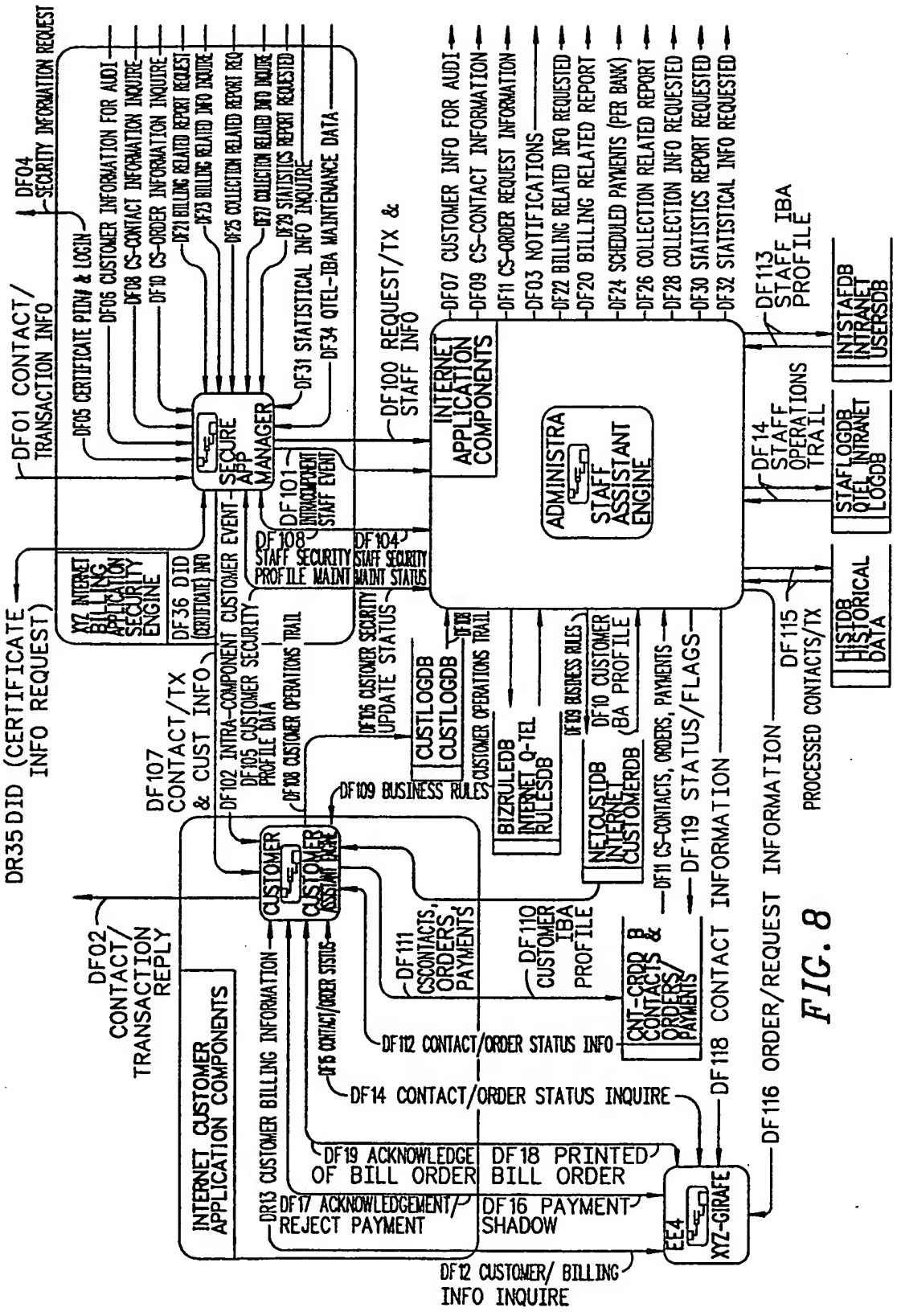

DR35 DID (CERTIFICATE INFO REQUEST)
DF01 CONTACT/ TRANSACTION INFO
DF04 SECURITY INFORMATION REQUEST
DF05 CERTIFICATE PIN/# & LOGIN
DF06 CUSTOMER INFORMATION FOR AUDI
DF08 CS-CONTACT INFORMATION INQUIRE
DF10 CS-ORDER INFORMATION INQUIRE
DF21 BILLING RELATED REPORT REQUEST
DF23 BILLING RELATED INFO INQUIRE
DF25 COLLECTION RELATED REPORT REQ
DF27 COLLECTION RELATED INFO INQUIRE
DF29 STATISTICS REPORT REQUESTED
DF31 STATISTICAL INFO INQUIRE
DF34 QTEL-IBA MAINTENANCE DATA
DF100 REQUEST/TX & STAFF INFO
DF07 CUSTOMER INFO FOR AUDI
DF09 CS-CONTACT INFORMATION
DF11 CS-ORDER REQUEST INFORMATION
DF03 NOTIFICATIONS
DF22 BILLING RELATED INFO REQUESTED
DF20 BILLING RELATED REPORT
DF24 SCHEDULED PAYMENTS (PER BANK)
DF26 COLLECTION RELATED REPORT
DF28 COLLECTION INFO REQUESTED
DF30 STATISTICS REPORT REQUESTED
DF32 STATISTICAL INFO REQUESTED
DF113 STAFF IBA PROFILE
INTSTAFDB INTRANET USERSDB
DF14 STAFF OPERATIONS TRAIL
STAFLOGDB QTEL INTRANET LOGDB
HISTDB HISTORICAL DATA
DF115 PROCESSED CONTACTS/TX
XYZ INTERNET BILLING APPLICATION SECURITY ENGINE
DF36 DID (CERTIFICATE) INFO
SECURE APP MANAGER
DF101 INTRACOMPONENT STAFF EVENT
DF108 STAFF SECURITY PROFILE MAINT
DF104 STAFF SECURITY MAINT STATUS
INTERNET APPLICATION COMPONENTS
ADMINISTRA
STAFF ASSISTANT ENGINE
DF107 CONTACT/TX & CUST INFO
DF102 INTRA-COMPONENT CUSTOMER EVENT
DF105 CUSTOMER PROFILE DATA
DF108 CUSTOMER OPERATIONS TRAIL
DF106 CUSTOMER SECURITY UPDATE STATUS
CUSTLOGDB
DF109 BUSINESS RULES
BIZRULEDB INTERNET Q-TEL RULESDB
NETCUSTDB INTERNET CUSTOMERDB
DF10 CUSTOMER BA PROFILE
DF119 STATUS/FLAGS
DF118 CONTACT INFORMATION
DF116 ORDER/REQUEST INFORMATION
CUSTOMER
CUSTOMER ASSISTANT
DF02 CONTACT/ TRANSACTION REPLY
INTERNET CUSTOMER APPLICATION COMPONENTS
DR13 CUSTOMER BILLING INFORMATION
DF15 CONTACT/ORDER STATUS
DF111 CSCONTACTS, ORDERS, PAYMENTS
DF110 CUSTOMER IBA PROFILE
CNT-CRDR & CONTACTS/ ORDERS/ PAYMENTS
DF11 CS-CONTACTS, ORDERS, PAYMENTS
DF112 CONTACT/ORDER STATUS INFO
DF14 CONTACT/ORDER STATUS INQUIRE
DF19 ACKNOWLEDGE OF BILL ORDER
DF18 PRINTED BILL ORDER
DF17 ACKNOWLEDGEMENT/ REJECT PAYMENT
DF16 PAYMENT SHADOW
EE4 XYZ-GIRAFE
DF12 CUSTOMER/ BILLING INFO INQUIRE

FIG. 8

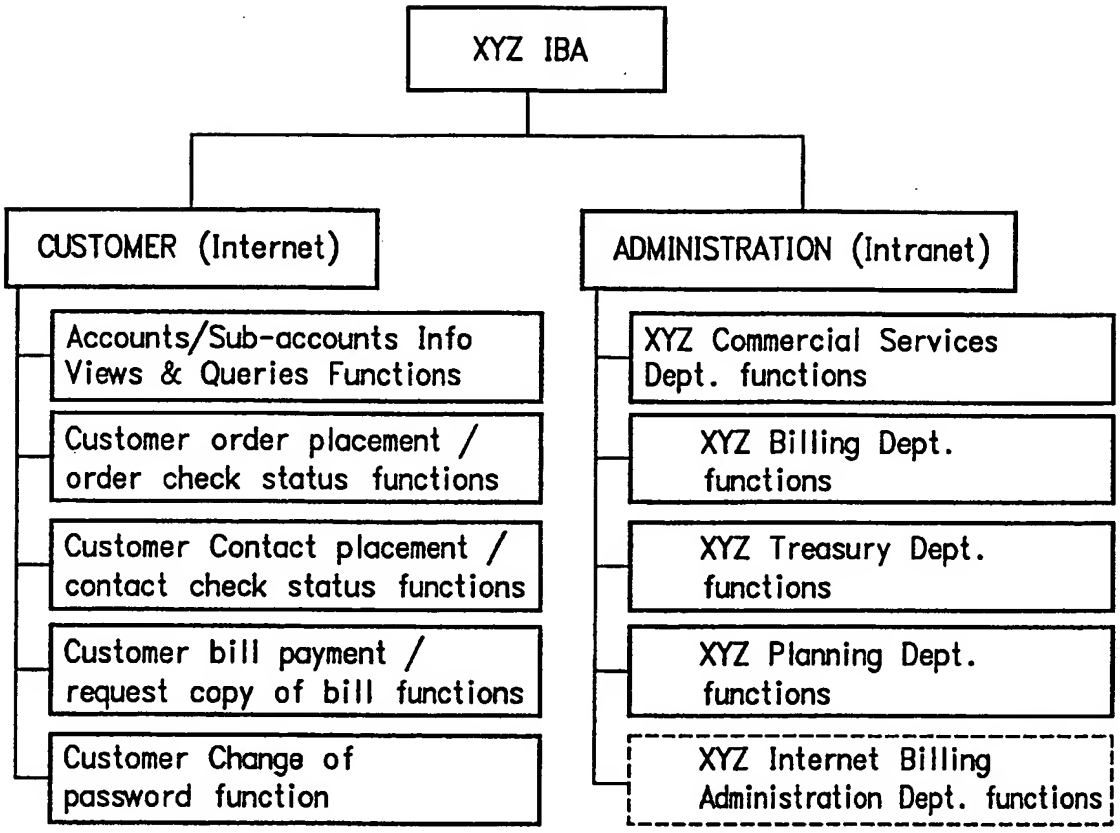

XYZ IBA
CUSTOMER (Internet)
ADMINISTRATION (Intranet)
Accounts/Sub-accounts Info Views & Queries Functions
Customer order placement / order check status functions
Customer Contact placement / contact check status functions
Customer bill payment / request copy of bill functions
Customer Change of password function
XYZ Commercial Services Dept. functions
XYZ Billing Dept. functions
XYZ Treasury Dept. functions
XYZ Planning Dept. functions
XYZ Internet Billing Administration Dept. functions

FIG. 9

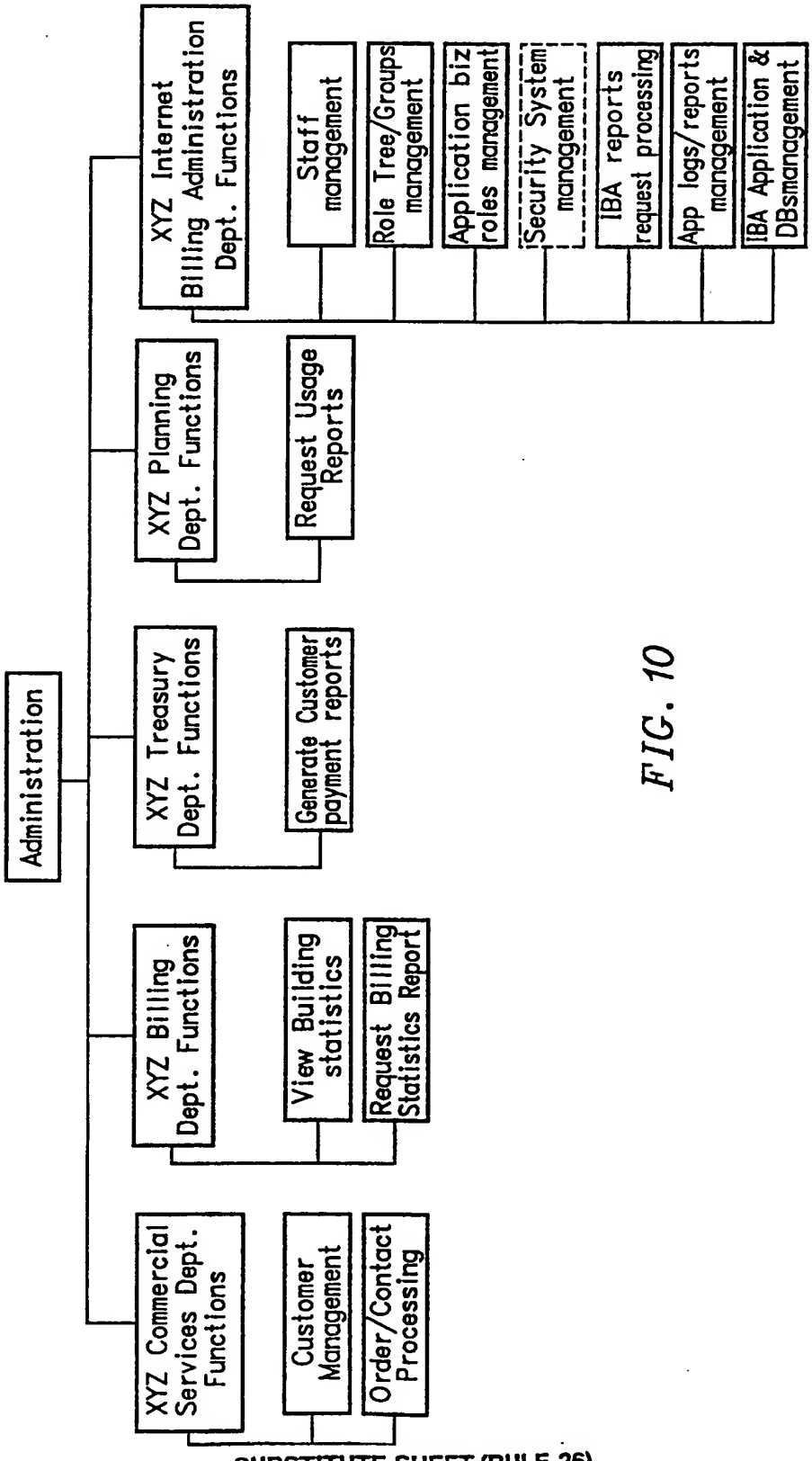

Administration
XYZ Internet Billing Administration Dept. Functions
Staff management
Role Tree/Groups management
Application biz roles management
Security System management
IBA reports request processing
App logs/reports management
IBA Application & DBsmanagement
XYZ Planning Dept. Functions
Request Usage Reports
XYZ Treasury Dept. Functions
Generate Customer payment reports
XYZ Billing Dept. Functions
View Building statistics
Request Billing Statistics Report
XYZ Commercial Services Dept. Functions
Customer Management
Order/Contact Processing

FIG. 10

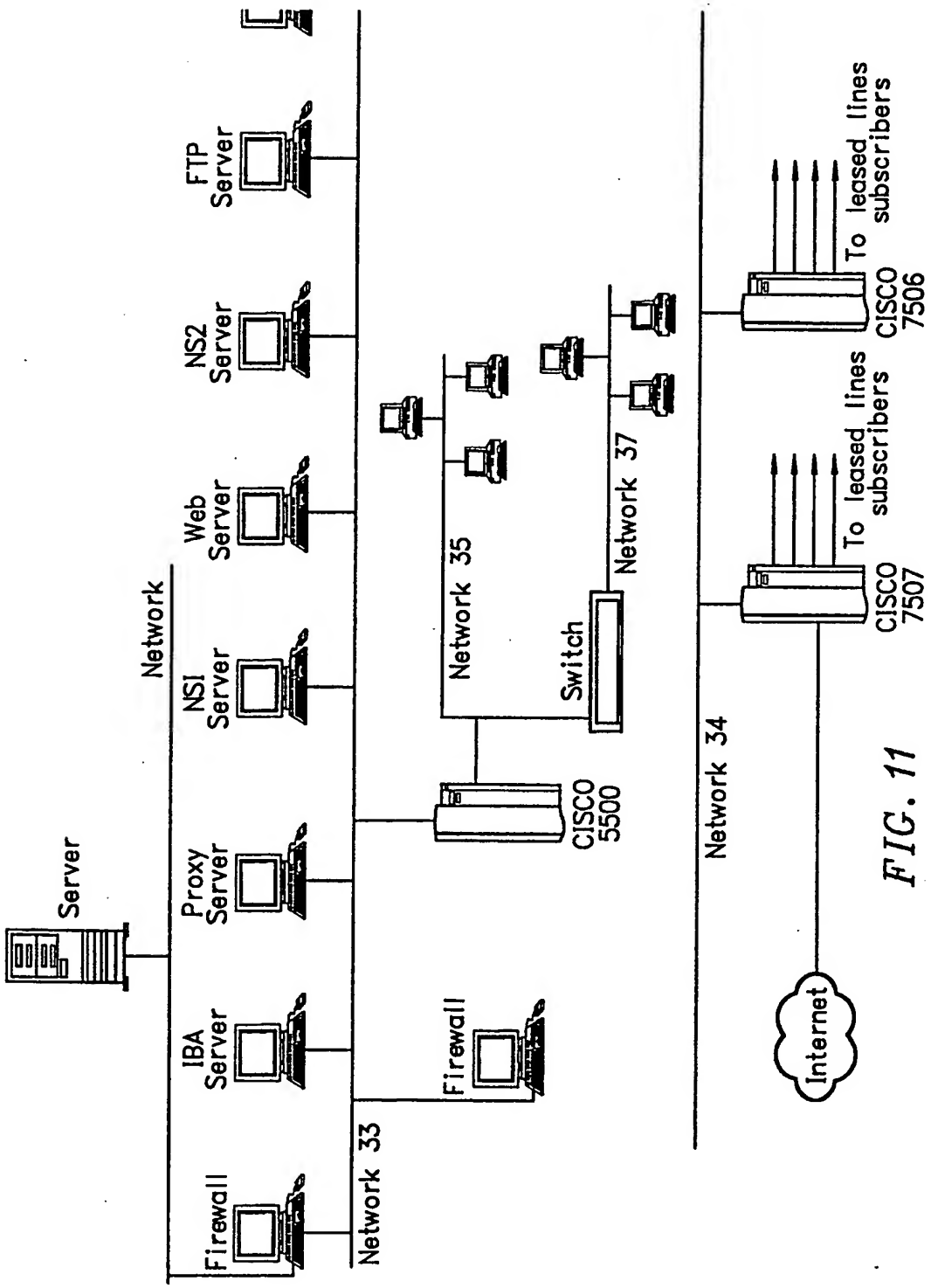

Server
Network
Proxy Server
NSI Server
Web Server
NS2 Server
FTP Server
IBA Server
Firewall
Network 33
Firewall
CISCO 5500
Network 35
Switch
Network 37
Network 34
CISCO 7507
CISCO 7506
To leased lines subscribers
To leased lines subscribers
Internet

FIG. 11

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10 | A3

(11) International Publication Number: WO 99/21319

(43) International Publication Date: 29 April 1999 (29.04.99)

(21) International Application Number: PCT/US98/22377

(22) International Filing Date: 21 October 1998 (21.10.98)

(30) Priority Data:
60/062,630 22 October 1997 (22.10.97) US
09/175,927 21 October 1998 (21.10.98) US

(71) Applicant: INTERX TECHNOLOGIES, INC. [US/US]; Suite H, 1805 Tribute Road, Sacramento, CA 95815 (US).

(72) Inventors: ABDALLAH, Wajdi; 5400 Garfield #46, Sacramento, CA 95841-2856 (US). DALMATOFF, Adam; 2765 Larkspur Lane, Sacramento, CA 95864 (US).

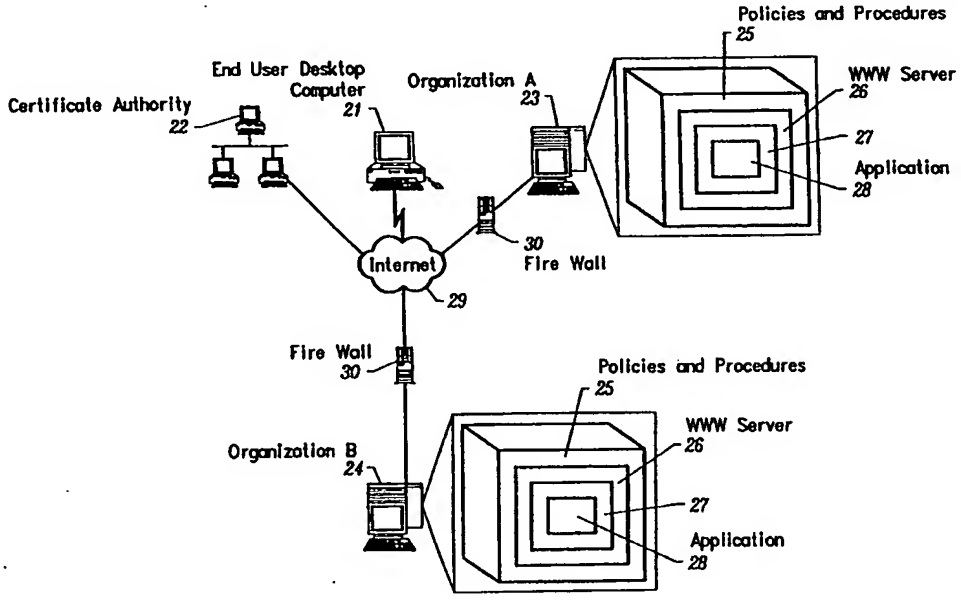
(74) Agents: GLENN, Michael, A. et al.; Law Offices of Michael A. Glenn, 125 Lake Road, Portola Valley, CA 94028 (US).

(81) Designated States: AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GD, GE, HR, HU, ID, IL, IS, JP, KP, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, UZ, VN, YU, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(88) Date of publication of the international search report:
24 June 1999 (24.06.99)

(54) Title: METHOD AND APPARATUS FOR CERTIFICATE MANAGEMENT IN SUPPORT OF NON-REPUDIATION



(57) Abstract

A non-repudiation mechanism for e-business is provided. E-business covers three areas: Intranet, Extranet, and E-commerce. The invention provides a link between a server which sends Internet requests to the requesting browser, and the application which houses the data and any computing functions. An audit trail is also provided to fix accountability. The invention controls the session between the server and the e-business application. The result is that each and every system request made via Internet technology can be correlated to a specific system user. Management utilities and reports provide the audit trail which provides non-repudiation (accountability).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

In ational Application No
PCT/US 98/22377

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 13013 A (OPEN MARKET INC) 2 May 1996	13,15, 16,29
A	see claim 1; figure 1	1-14, 17-28,30
A	WO 97 16798 A (MASTERCARD INTERNATIONAL INC) 9 May 1997 see claim 1; figure 1	1-30
A	WO 96 29667 A (SANDBERG DIMENT ERIK) 26 September 1996 see claim 1; figure 1	1-30
A	EP 0 801 479 A (AT & T CORP) 15 October 1997 see claim 1; figure 1	1-30

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 April 1999	21/04/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Ir. ational Application No
PCT/US 98/22377

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 613 012 A (HOFFMAN NED ET AL) 18 March 1997 see claim 1; figure 1	1-30

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/22377

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9613013 A	02-05-1996	US 5715314 A	03-02-1998
		EP 0803105 A	29-10-1997
		JP 10509543 T	14-09-1998
WO 9716798 A	09-05-1997	US 5699528 A	16-12-1997
		AU 7722996 A	22-05-1997
		CA 2236432 A	09-05-1997
		EP 0859983 A	26-08-1998
WO 9629667 A	26-09-1996	US 5826245 A	20-10-1998
		AU 5366096 A	08-10-1996
EP 0801479 A	15-10-1997	CA 2193748 A	30-06-1997
		JP 10031634 A	03-02-1998
US 5613012 A	18-03-1997	US 5615277 A	25-03-1997
		AU 5922696 A	29-11-1996
		BR 9608580 A	05-01-1999
		CA 2221321 A	21-11-1996
		CN 1191027 A	19-08-1998
		WO 9636934 A	21-11-1996
		US 5838812 A	17-11-1998
		US 5870723 A	09-02-1999
		US 5764789 A	09-06-1998
		US 5802199 A	01-09-1998
		US 5805719 A	08-09-1998